ON PAIRS OF p-ADIC ANALOGUES OF THE CONJECTURES OF BIRCH AND SWINNERTON-DYER

by

Florian Sprung

Abstract. — For a weight two modular form and a good prime p, we construct a vector of Iwasawa functions $(L_p^\sharp, L_p^\flat)$. In the elliptic curve case, we use this vector to put the p-adic analogues of the conjectures of Birch and Swinnerton-Dyer for ordinary [**MTT**] and supersingular [**BPR**] primes on one footing. Looking at $L_p^\sharp$ and $L_p^\flat$ individually leads to a stronger conjecture containing an extra zero phenomenon.

We also give an explicit upper bound for the analytic rank in the cyclotomic direction and an asymptotic formula for the p-part of the analytic size of the Šafarevič-Tate group in terms of the Iwasawa invariants of $L_p^\sharp$ and $L_p^\flat$. A very puzzling phenomenon occurs in the corresponding formulas for modular forms. When p is supersingular, we prove that the two classical p-adic L-functions ([**AV75**],[**Vi76**]) have finitely many common zeros, as conjectured by Greenberg.

Contents

Introduction

The principal aim of this article is to construct a vector $(L_p^\sharp, L_p^\flat)$ of p-adic L-functions for modular forms of weight two and primes p of good reduction. The functions $L_p^\sharp$ and $L_p^\flat$ are elements of the Iwasawa algebra $\Lambda = \ _p[[T]]$, and thus shed light on various arithmetic questions,

Key words and phrases. — Birch and Swinnerton-Dyer, p-adic L-function, elliptic curve, modular form, Šafarevič-Tate group, Iwasawa Theory. Ą@11G40 (primary), 11F67 (secondary), 11R23, 11G05.

including a formulation of a new p-adic version of the conjectures of Birch and Swinnerton-Dyer, unifying and generalizing the questions for ordinary and supersingular primes, which have traditionally been treated separately.

To keep the introduction simple, let p be for now an odd prime at which a fixed elliptic curve $E/\mathbb{Q}$ has good reduction. When p is *ordinary*, Mazur and Swinnerton-Dyer ([**MSD**], [**Ma71**]) constructed *one* p-adic L-function $L_p(E,T)$ (which should live in Λ), whose behavior at special values can be conjecturally related to arithmetic invariants of the elliptic curve. In the *supersingular* case, the analogous questions typically involved p-adic L-functions $L_p(E,\alpha,T)$ and $L_p(E,\beta,T)$ ([**AV75**],[**Vi76**]) which are power series with unbounded coefficients and thus not elements of Λ. Thanks to [**Ko03**],[**Po03**],[**Sp12**], they can be rewritten as linear combinations of a *pair* $L_p^\sharp$ and $L_p^\flat$ of functions in Λ. Reworking the construction of the classical p-adic L-functions *in vitro*, we give a natural extension of this decomposition to include the ordinary case, so that we can express Mazur/Swinnerton-Dyer's $L_p(E,T)$ as a linear combination of an appropriate pair $L_p^\sharp$ and $L_p^\flat$ as well. Thus, the essential p-adic analytic information is contained in our pair $L_p^\sharp, L_p^\flat$, *whether p is ordinary or supersingular.*

Our pair $L_p^\sharp = L_p^\sharp(E,T)$ and $L_p^\flat = L_p^\flat(E,T)$ is related to the classical p-adic L-functions much like the completed Riemann zeta function is related to the original zeta function. The analogue of the Gamma factor is the matrix

$$\mathcal{L}og_{\alpha,\beta}(1+T) := \lim_{n\to\infty} \mathcal{C}_1\cdots\mathcal{C}_n C^{-(n+2)}\begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix}, \text{ where}$$

$\mathcal{C}_i := \begin{pmatrix} a_p & 1 \\ -\Phi_{p^i}(1+T) & 0 \end{pmatrix}$, $C := \begin{pmatrix} a_p & 1 \\ -p & 0 \end{pmatrix}$, α and β are the eigenvalues of Frobenius and $a_p = \alpha+\beta$ is the trace, and $\Phi_n(X)$ is the nth cyclotomic polynomial.

The entries of this matrix are p-adic analytic functions when p is supersingular, and we generalize a theorem of Pollack [**Po03**] (who assumed $a_p = 0$):

$$(L_p(E,\alpha,T), L_p(E,\beta,T)) = (L_p^\sharp(E,T), L_p^\flat(E,T))\mathcal{L}og_{\alpha,\beta}(1+T),$$

where $(L_p^\sharp(E,T), L_p^\flat(E,T)) \in \Lambda^{\oplus 2}$.

In the ordinary case, the first column $\begin{pmatrix} \log_\alpha^\sharp \\ \log_\alpha^\flat \end{pmatrix}$ of $\mathcal{L}og_{\alpha,\beta}$ is defined and consists of p-adically analytic functions. We have $(L_p^\sharp, L_p^\flat) \in \Lambda^{\oplus 2}$ when $a_p \not\equiv 1 \mod p$,[1] and

$$L_p(E,T) = L_p^\sharp \log_\alpha^\sharp + L_p^\flat \log_\alpha^\flat .$$

Equipped with our pair $L_p^\sharp, L_p^\flat$, we conjecturally relate arithmetic invariants of E to analytic invariants of the *vector* $(L_p^\sharp(E,T), L_p^\flat(E,T))$ coming from its behavior at $T=0$. Because of the above relations to the classical p-adic L-functions, this p-adic version of BSD is equivalent to the conjecture of Mazur, Tate, and Teitelbaum (who worked with $L_p(E,T)$) when p is

[1] In the excluded case, they live in $(\mathbb{Q}\otimes\Lambda)^{\oplus 2}$.

ordinary, and to that of Bernardi and Perrin-Riou (who essentially worked with $L_p(E,\alpha,T)$ and $L_p(E,\beta,T)$) when p is supersingular, giving a uniform treatment of their conjectures. But we can generalize this conjecture by asking what the order of zero of *each function* $L_p^\sharp(E,T)$ and $L_p^\flat(E,T)$ tells us about the rank of $E(\mathbb{Q})$. Here, we find a puzzling phenomenon: when $a_p = 2$ (resp. when $p = 2$ and $a_2 = 1$), the order of vanishing of $L_p^\sharp(E,T)$ (resp. $L_p^\flat(E,T)$) should be *larger* than the rank of $E(\mathbb{Q})$. This exceptional zero phenomenon is reminiscent of that of the p-adic L-function in the split multiplicative case, but we have not found any conceptual reason that adequately explains it.

We also construct a completed version $\widehat{\mathcal{L}og}_{\alpha,\beta}$ of $\mathcal{L}og_{\alpha,\beta}$, and similarly $\widehat{L}_p^\sharp$ and $\widehat{L}_p^\flat$, and then prove functional equations for these completed objects. We derive functional equations for $L_p^\sharp$ and $L_p^\flat$ in some cases as well. They correct a corresponding statement in [**Po03**] (where $a_p = 0$), which is off by a unit factor. The algebraic version of the functional equation by Kim [**Ki08**] when $a_p = 0$ is still correct, since it is given up to units. It would be interesting to generalize Kim's theorem to the case $a_p \neq 0$.

In the supersingular case, Greenberg asked in [**Gr01**] whether $L_p(E,\alpha,T)$ and $L_p(E,\beta,T)$ have finitely many common zeros. Building on works of Rohrlich, Pollack has proved this conjecture in the case $a_p = 0$ in [**Po03**]. As a corollary to our methods, we give another proof that works for any supersingular prime (and in fact for any weight two modular form) and thus settles Greenberg's conjecture.

We can bound the analytic rank of the elliptic curve (the rank as predicted by BSD) as one climbs up the cyclotomic $_p$-extension: In the case $a_p = 0$, we prove that an upper bound is the sum $\lambda_\sharp + \lambda_\flat$ of the λ-invariants of $L_p^\sharp$ and $L_p^\flat$, which generalizes works of Pollack (who assumed further that $p \equiv 3 \mod 4$), before giving a different bound of the form λ_*+(p-power sum) for an appropriate $* \in \{\sharp, \flat\}$ that includes the case $a_p \neq 0$ as well. In the ordinary case, the p-power sum is zero. In the supersingular case, this upper bound may be larger or smaller than $\lambda_\sharp + \lambda_\flat$, and there are cases when $a_p \neq 0$ in which the bound $\lambda_\sharp + \lambda_\flat$ fails. Thus, an interesting question to ask is: What is the best bound?

We then pose a conjecture that gives arithmetic significance to the greatest common divisor of $L_p^\sharp$ and $L_p^\flat$, generalizing a conjecture of Kurihara and Pollack (who worked in the case $a_p = 0$), and show how a cyclotomic version of p-adic *BSD* would imply a divisibility toward this conjecture.

After that, we scrutinize the special value at 1 of the complex L-function twisted at various p-power characters in terms of the Iwasawa invariants of $L_p^\sharp$ and $L_p^\flat$. By the cyclotomic version of BSD, these values should correspond to the size of the Šafarevič-Tate group Ш in the cyclotomic direction. We derive growth patterns for the p-part of the expected size of Ш along the cyclotomic $_p$ extension, making no assumption other than that p is of good reduction. The most involved scenario occurs when $a_p = \pm p$, where we encounter *three* possible patterns. This part of the paper was originally a twin to [**Sp13**], in which we have given an algebraic version of this theorem for an odd prime p in the supersingular case in terms of Iwasawa invariants coming from $\sharp/\flat$-Selmer groups, generalizing work of Kobayashi (who assumed $a_p = 0$, and thus in turn gave an algebraic version of a theorem by Pollack). Our formulas also match the algebraic ones of Kurihara and Otsuki for the case $p = 2$ [**KO06**]. For the unknown cases (in which $p = 2$), we therefore obtain a prediction of how Ш grows.

A very mysterious phenomenon occurs when we do the corresponding computations for a modular form of weight two, whose coefficients need not be rational. We obtain formulas for the growth of the special value depending not only on the Iwasawa invariants $\mu_\sharp, \mu_\flat, \lambda_\sharp, \lambda_\flat$, but also on the normalized valuation $v = \mathrm{ord}_p(a_p)$: There is a formula for each of infinitely many intervals (that become arbitrarily small) inside which v lies. These formulas are continuous in v: In particular if v approaches zero, these formulas converge toward those for the ordinary case. During this voyage toward zero, the roles of $\sharp$ and $\flat$ also change infinitely often. When $\mu_\sharp \neq \mu_\flat$, the formulas depend, at some critical values of v (including those at which this role switch occurs), also on the valuation of yet another element v_2, in which they are also continuous. It is a complete mystery why these formulas appear in this way, but we illustrate this puzzling phenomenon with a picture.

In the supersingular case, Greenberg, Iovita, and Pollack (in unpublished work around 2005) generalized the approach of Perrin-Riou of extracting invariants $\mu_\pm$ and $\lambda_\pm$ from the classical p-adic L-functions for a modular form f, $L_p(f, \alpha, T)$ and $L_p(f, \beta, T)$, which they used for their estimates (under the assumption $\mu_+ = \mu_-$). Our formulas match theirs exactly in those cases, although the techniques are completely different.

0.1. Organization of Paper. — In Section 2, we introduce *Mazur-Tate symbols*, which inherit special values of L-functions, to construct the classical p-adic L-functions of Amice, Vélu, and Višik. In Section 3, we define the logarithm matrix $\mathcal{L}og_{\alpha,\beta}$ and prove its basic properties. In Section 4, we then put this information together to rewrite the p-adic L-functions from Section 2 in terms of the new p-adic L-functions $L_p^\sharp$ and $L_p^\flat$. We then go on to answer the question posed by Greenberg in Section 4. In Section 5, we recall the two p-adic versions of the conjectures of Birch and Swinnerton-Dyer, for the ordinary and the supersingular case, and state our conjectures. Section 6 is devoted to the BSD-theoretic aspects as one climbs up the cyclotomic tower.

0.2. Outlook. — Lei, Loeffler, and Zerbes have used the theory of *Wach modules* to construct pairs of p-adic L-functions in $\Lambda \otimes \mathbb{Q}$: They are power series whose coefficients have bounded growth. Their analogue of $\mathcal{L}og_{\alpha,\beta}(1+T)$ is not constructed directly, so that one might ask: How are the matrices related? Should their p-adic L-functions be in Λ like ours? In [**LLZ10**], these issues are addressed, but not solved explicitly. Their construction has the advantage of working for higher weight as well, as long as a_p is close enough to 0 to allow for the Wach module basis constructed in [**BLZ**]. For the ordinary p-adic L-function, [**LLZ10**] and [**LZ**]'s construction also gives rise to an analogue of $\mathcal{L}og_{\alpha,\beta}$ in the ordinary case, from which they construct a companion p-adic L-function, the critical slope p-adic L-function of Kato and Perrin-Riou. Note that they give a *separate* construction for the Wach module in the ordinary case. Here, the obvious question to ask is how the first column of their matrix is related to the first column of $\mathcal{L}og_{\alpha,\beta}$, and whether the second column of $\mathcal{L}og_{\alpha,\beta}$ converges - if it did, that would give rise to a (more explicit) companion p-adic L-function. Another question is how these companion p-adic L-functions are related to that of [**PoSt**]. A trace of the companion can be found in the proofs throughout our paper whenever we make use of the fact that the second column of $\mathcal{L}og_{\alpha,\beta}(1+T)$ converges at specific values, including $T = 0$. Another question is what a Main Conjecture in terms of $L_p^\sharp$ and $L_p^\flat$ looks like. A proof of the Main Conjecture in terms of $L_p(E,T)$, stating that it generates an appropriate characteristic Λ-ideal of E is due to [**SU**], building on [**Ka04**]. See also [**Ru91**] for the CM case.

For the higher weight case, there are generalizations of $L_p^\sharp$ and $L_p^\flat$, which is forthcoming work in [**Sp**]. Their invariants are already sometimes visible (see e.g. [**PW11**]). It would be nice to generalize the pairs of p-adic BSD conjectures to modular abelian varieties as well. For the ordinary reduction case, the generalization of [**MTT**] is [**BMS**]. Another challenge is formulating p-adic BSD for a prime of bad reduction. Apart from [**MTT**], a hint for what to do can be found in Delbourgo's formulation of Iwasawa theory [**De98**].

1. The p-adic L-function of a modular form

In this section, we recall the classical p-adic L-functions given in [**AV75**], [**MTT**], [**Vi76**], and [**MSD**], in the case of weight two modular forms. We give a construction from the point of view of **queue sequences**, so that we can rewrite them later *in vitro* as linear combinations of p-adic L-functions $L_p^\sharp$ and $L_p^\flat$. This is the most important theorem of this paper, which will be proved in the Sections 2 and 3, and upon which the applications (Sections 4-6) depend.

Let f be a weight two modular form with character ϵ which is an eigenform for the Hecke operators T_n with eigenvalue $a_n, K(f)$ the number field $\mathbb{Q}((a_n)_{n\in\mathrm{N}}, \epsilon(\quad))$ and its ring of integers. We also fix forever a prime p of good reduction. Given integers a, m, the *period* of f is

$$\varphi\left(f, \frac{a}{m}\right) := 2\pi i \int_{i\infty}^{\frac{a}{m}} f(z)dz.$$

The following theorem fortunately puts these transcendental periods in the algebraic realm.

Theorem 1.1. — *There are nonzero complex numbers $\Omega_f^\pm$ so that the following expressions are both in :*

$$\left[\frac{a}{m}\right]_f^+ := \frac{\varphi(f,\frac{a}{m})+\varphi(f,\frac{-a}{m})}{2\Omega_f^+} \text{ and } \left[\frac{a}{m}\right]_f^- := \frac{\varphi(f,\frac{a}{m})-\varphi(f,\frac{-a}{m})}{2\Omega_f^-}.$$

Proof. — [**Ma73**, Theorem 1.2], [**Sh77**, Theorem 1], or [**GS94**, Theorem 3.5.4].

$\left[\frac{a}{m}\right]_f^\pm$ are called *modular symbols.* They allow us to construct p-adic L-functions as follows: Denote by $\ ^0(\ {}^\times_p)$ the ${}_p$-valued step functions on ${}^\times_p$. Let a be an integer prime to p, and denote by ${}_U$ the characteristic function of an open set U. We let ord_p be the valuation associated to p so that $\mathrm{ord}_p(p)=1$. Denote by α and β the roots of the Hecke polynomial $X^2-a_pX+\epsilon(p)p$ of the modular form f so that $\mathrm{ord}_p(\alpha)<1$. We define a linear map $\mu_{f,\alpha}^\pm$ from $\ ^0(\ {}^\times_p)$ to ${}_p$ by setting for a coprime to p:

$$\mu_{f,\alpha}^\pm(\ {}_{a+p^n\mathbb{Z}_p}) = \frac{1}{\alpha^{n+1}}\left(\left[\frac{a}{p^n}\right]_f^\pm, \left[\frac{a}{p^{n-1}}\right]_f^\pm\right)\begin{pmatrix}\alpha\\ -\epsilon(p)\end{pmatrix}.$$

Remark 1.2. — The maps $\mu_{f,\alpha}^\pm$ are not measures, but $\mathrm{ord}_p(\alpha)$-admissible measures. See e.g. [**Po03**]. For background on measures, see [**Wa80**, Section 12.2].

Theorem 1.3. — *We can extend the maps $\mu_{f,\alpha}^\pm$ to all analytic functions on ${}^\times_p$.*

This is done by locally approximating analytic functions by *step functions*, since $\mu_{f,\alpha}^\pm$ are $\mathrm{ord}_p(\alpha)<1$-admissible measures. That is, we look at their Taylor series expansions and ignore the higher order terms. For an explicit construction, see [**AV75**] or [**Vi76**]. Since characters χ of ${}^\times_p$ are locally analytic functions, we thus obtain an element

$$L_p(f,\alpha,\chi) := \mu_{f,\alpha}^{\mathrm{sign}(\chi)}(\chi).$$

Now since ${}^\times_p \cong (\ /2p\ )^\times \times (1+2p\ {}_p)$, we can write a character χ on ${}^\times_p$ as a product

$$\chi = \omega^i\chi_u$$

with $0 \leqslant i < |\Delta|$ for some $u \in\ {}_p$ with $|u-1|_p<1$, where χ_u sends sends the topological generator $\gamma=1+2p$ of $1+2p\ {}_p$ to u, and where $\omega:\Delta\to\ {}^\times_p \in\ {}_p$ is the usual embedding of the $|\Delta|$-th roots of unity in ${}_p$ so that ω^i is a tame character of $\Delta=(\ /2p\ )^\times$. Using this product, we can identify the open unit disk of ${}_p$ with characters χ on ${}^\times_p$ having the same tame character ω^i. Thus if we fix i, we can regard $L_p(f,\alpha,\omega^i\chi_u)$ as a function on the open unit disk. We can go even further:

Theorem 1.4 ([**Vi76**], [**MTT**], [**AV75**], [**Po03**]). — *Fix a tame character $\omega^i:\Delta=(\ /2p\ )^\times\to\ {}_p$. Then the function $L_p(f,\alpha,\omega^i\chi_u)$ is an analytic function converging on the open unit disk.*

We can thus form its power series expansion about $u=1$. For convenience, we change variables by setting $T=u-1$ and denote $L_p(f,\alpha,\omega^i\chi_u)$ by $L_p(f,\alpha,\omega^i,T)$. If $i=0$ so that $\omega^i=\ $ is the trivial character, we denote this function simply by $L_p(f,\alpha,T)$.

Denote by $\zeta = \zeta_{p^n}$ a primitive p^nth root of unity. We can then regard $\omega^i\chi_\zeta$ as a character of $(\quad/p^N\quad)^\times$, where $N = n+1$ if p is odd and $N = n+2$ if $p = 2$. Given any character ψ of $(\quad/p^N\quad)^\times$, let $\tau(\psi)$ be the Gauß sum $\sum_{a\in(\mathbb{Z}/p^N\mathbb{Z})^\times}\psi(a)\zeta_{p^N}^a$. Then we have:

Theorem 1.5 **([Vi76], [MTT], [AV75], [Po03])**. — *(Amice-Vélu, Višik)*

$$L_p(f,\alpha,0) = \left(1-\frac{1}{\alpha}\right)^2\frac{L(f,1)}{\Omega_f^+} \text{ and } L_p(f,\alpha,\omega^i,\zeta-1) = \frac{1}{\alpha^N}\frac{p^N}{\tau\left(\omega^{-i}\chi_{\zeta^{-1}}\right)}\frac{L\left(f_{\omega^{-i}\chi_{\zeta^{-1}}},1\right)}{\Omega_f^{\omega^i(-1)}}.$$

1.1. Queue sequences and Mazur-Tate elements. — Denote by μ_{p^n} the group of p^nth roots of unity, and put $\mathcal{G}_N := \mathrm{Gal}(\mathbb{Q}(\mu_{p^N}))$. We let $\mathbb{Q}_n$ be the unique subextension of $\mathbb{Q}(\mu_{p^N})$ with Galois group isomorphic to $\quad/p^n\quad$ and put $\Gamma_n := \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$. We also let $\Gamma := \mathrm{Gal}(\bigcup_n \mathbb{Q}_n/\mathbb{Q})$. We then have an isomorphism

$$\mathcal{G}_N \cong \Delta\times\Gamma_n.$$

Let $\Lambda_n = \ [\Gamma_n]$ be the finite version of the Iwasawa algebra at level n. We need two maps $\nu = \nu_{n-1/n}$ and $\pi = \pi_{n/n-1}$ to construct **queue sequences**: π is the natural projection from Λ_n to Λ_{n-1}, and the map $\Lambda_n \xrightarrow{\nu_{n-1/n}} \Lambda_{n-1}$ we define by $\nu_{n-1/n}(\sigma) = \sum_{\tau\mapsto\sigma,\tau\in\Gamma_n}\tau$. We let $\Lambda = \ [[\Gamma]] = \varprojlim_{\pi_{n/n-1}}\ [\Gamma_n]$ be the Iwasawa algebra. We identify Λ with $\ [[T]]$ by sending our topological generator $\gamma = 1+2p$ of $\Gamma \cong \ _p$ to $1+T$. This induces an isomorphism between Λ_n and $\ [[T]]/((1+T)^{p^n}-1)$.

Definition 1.6. — A **queue sequence** is a sequence of elements $(\Theta_n)_n \in (\Lambda_n)_n$ so that

$$\pi\Theta_n = a_p\Theta_{n-1} - \epsilon(p)\nu\Theta_{n-2} \text{ when } n \geqslant 2.$$

Definition 1.7. — For $a \in \mathcal{G}_N$, denote its projection onto Δ by $\overline{a}$, and let $i : \Delta \hookrightarrow \mathcal{G}_N$ be the standard inclusion, so that $\frac{a}{i(\overline{a})} \in \Gamma_n$. Define $\log_\gamma(a)$ to be the smallest positive integer so that the image of $\gamma^{\log_\gamma(a)}$ under the projection from Γ to Γ_n equals $\frac{a}{i(\overline{a})}$. We then have a natural map $i : \Delta \hookrightarrow \mathcal{G}_\infty$ which allows us to extend this definition to any $a \in \mathcal{G}_\infty = \varprojlim_N \mathcal{G}_N$: Let $\log_\gamma(a)$ be the unique element of $\ _p^\times$ so that $\gamma^{\log_\gamma(a)} = \frac{a}{i(\overline{a})}$.

Example 1.8. — *We make the identification $\mathcal{G}_N \cong (\quad/p^N\quad)^\times$ by identifying σ_a with a, where $\sigma_a(\zeta) = \zeta^a$ for $\zeta \in \mu_{p^N}$. This allows us to construct the **Mazur-Tate element**, which is the following element:*

$$\vartheta_N^\pm := \sum_{a\in(\mathbb{Z}/p^N)^\times}\left[\frac{a}{p^N}\right]_f^\pm \sigma_a \in \ [\mathcal{G}_N].$$

For each character $\omega^i : \Delta \to \ _p^\times$, put

$$\varepsilon_{\omega^i} = \frac{1}{\#\Delta}\sum_{\tau\in\Delta}\omega^i(\tau)\tau^{-1}.$$

We can take isotypical components $\varepsilon_{\omega^i}\vartheta_N$ of the Mazur-Tate elements, which can be regarded as elements of $\Lambda_n \cong [[T]]/((1+T)^{p^n}-1)$. Denote these ***Mazur-Tate elements associated to the tame character*** *ω^i by*

$$\theta_n(\omega^i,T) := \varepsilon_{\omega^i}\vartheta_N^{\mathrm{sign}(\omega^i)}.$$

We extend ω^i to all of $(\ /p^N \ )^\times$ by precomposing with the natural projection onto Δ, and can thus write these elements explicitly as elements of Λ_n:

$$\theta_n(\omega^i,T) = \sum_{a\in(\mathbb{Z}/p^N\mathbb{Z})^\times} \left[\frac{a}{p^N}\right]_f^{\mathrm{sign}(\omega^i)} \omega^i(a)(1+T)^{\log_\gamma(a)}.$$

When $\omega^i = \quad$ is the trivial character, we simply write $\theta_n(T)$ instead of $\theta_n(\ ,T)$. For a fixed tame character ω^i, the associated Mazur-Tate elements $\theta_n(\omega^i,T)$ form a queue sequence. For a proof, see [**MTT**, (4.2)].

We can now explicitly approximate $L_p(f,\alpha,\omega^i,T)$ by Riemann sums:

Definition 1.9. — Put

$$L_{N,\alpha}^{\pm} := \sum_{a\in(\mathbb{Z}/p^N\mathbb{Z})^\times} \mu_{f,\alpha}^{\pm}(\ _{a+p^N\mathbb{Z}_p})\sigma_a \in \ _p[\mathcal{G}_N],$$

so we get the representation

$$\varepsilon_{\omega^i}L_{N,\alpha}^{\mathrm{sign}(\omega^i)}(T) = \sum_{a\in(\mathbb{Z}/p^N\mathbb{Z})^\times} \mu_{f,\alpha}^{\mathrm{sign}(\omega^i)}(\ _{a+p^n\mathbb{Z}_p})\omega^i(a)(1+T)^{\log_\gamma(a)}.$$

Note that the homomorphism $\nu:\Gamma_n\to\Gamma_{n+1}$ extends naturally to a homomorphism from $\mathcal{G}_N$ to $\mathcal{G}_{N+1}$, also denoted by ν.

Lemma 1.10. — *Let $n\geqslant 0$, i.e. $N\geqslant 1$ for odd p, and $N\geqslant 2$ for $p=2$. Then*

$$(L_{N,\alpha}^{\pm}, L_{N,\beta}^{\pm}) = (\vartheta_N^{\pm}, \nu\vartheta_{N-1}^{\pm})\begin{pmatrix} \alpha^{-N} & \beta^{-N} \\ -\epsilon(p)\alpha^{-(N+1)} & -\epsilon(p)\beta^{-(N+1)} \end{pmatrix}.$$

Proof. — From the definitions. *QED*

Proposition 1.11. — *As functions converging on the open unit disk, we have*

$$L_p(f,\alpha,\omega^i,T) = \lim_{n\to\infty}\varepsilon_{\omega^i}L_{N,\alpha}^{\mathrm{sign}(\omega^i)}(T).$$

Proof. — Approximation by Riemann sums, and decomposition into tame characters. *QED*

Corollary 1.12. — *Let p be supersingular. Then both α and β have valuation strictly less than one, so we can reconstruct the p-adic L-functions by the Mazur-Tate elements:*

$$\big(L_p(f,\alpha,\omega^i,T), L_p(f,\beta,\omega^i,T)\big) = \lim_{n\to\infty}(\theta_n(\omega^i,T),\nu\theta_{n-1}(\omega^i,T))\begin{pmatrix} \alpha^{-N} & \beta^{-N} \\ -\epsilon(p)\alpha^{-(N+1)} & -\epsilon(p)\beta^{-(N+1)} \end{pmatrix}$$

In the ordinary case, we have $\mathrm{ord}_p(\alpha)=0<1$, *so*

$$L_p(f,\alpha,\omega^i,T) = \lim_{n\to\infty}(\theta_n(\omega^i,T),\nu\theta_{n-1}(\omega^i,T))\begin{pmatrix} \alpha^{-N} \\ -\epsilon(p)\alpha^{-(N+1)} \end{pmatrix}.$$

Proof. — This follows from Lemma 1.10. *QED*

These Mazur-Tate elements are so conveniently behaved that we can rewrite the limit in the above corollary to arrive at the main theorem in the paper:

Theorem 1.13. — *There is a vector of two Iwasawa functions* $\left(\widehat{L}_p^\sharp(f,\omega^i,T),\widehat{L}_p^\flat(f,\omega^i,T)\right)\in\Lambda^{\oplus 2}$ *for each tame character* ω^i *and a* 2×2*-matrix* $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ *with entries convergent in the open unit disk when p is supersingular, and whose first column entries converge when p is ordinary, so that*

$$\begin{cases}\left(L_p(f,\alpha,\omega^i,T),L_p(f,\beta,\omega^i,T)\right)=\left(\widehat{L}_p^\sharp(f,\omega^i,T),\widehat{L}_p^\flat(f,\omega^i,T)\right)\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T) \text{ for supersingular } p\\ L_p(f,\alpha,\omega^i,T)=\left(\widehat{L}_p^\sharp(f,\omega^i,T),\widehat{L}_p^\flat(f,\omega^i,T)\right)\left(\begin{smallmatrix}\widehat{\log}_\alpha^\sharp(1+T)\\ \widehat{\log}_\alpha^\flat(1+T)\end{smallmatrix}\right) \text{ for ordinary } p,\end{cases}$$

where $\left(\begin{smallmatrix}\widehat{\log}_\alpha^\sharp(1+T)\\ \widehat{\log}_\alpha^\flat(1+T)\end{smallmatrix}\right)$ *is the first column of* $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$.

An analogous statement with objects without the hats holds.

The construction and analysis of $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ occupies Section 2, and that of the two Iwasawa functions $\left(\widehat{L}_p^\sharp(f,\omega^i,T),\widehat{L}_p^\flat(f,\omega^i,T)\right)$ Section 3.

2. The logarithm matrix $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$

2.1. Definition of the matrix $\mathcal{L}og_{\alpha,\beta}(1+T)$. — In this section, we construct a matrix $\mathcal{L}og_{\alpha,\beta}(1+T)$ whose entries are functions converging on the open unit disk in the supersingular case. In the ordinary case, its first column converges. They generalize the four functions $\log_{\alpha/\beta}^{\sharp/\flat}$ from [**Sp12**] and also the three functions $\log_p^+,\log_p^-\cdot\alpha,\log_p^-\cdot\beta$ from [**Po03**]. We also construct a completed version $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$.

Definition 2.1. — Let $i\geqslant 1$. We *complete* the p^ith cyclotomic polynomial by putting

$$\widehat{\Phi}_{p^i}(1+T):=\Phi_{p^i}(1+T)/(1+T)^{\frac{1}{2}p^{i-1}(p-1)},$$

except when $p=2$ and $i=1$: To avoid branch cuts (square roots), we set

$$\widehat{\Phi}_2(1+T):=\Phi_2(1+T).$$

Definition 2.2. — Define the following matrix:

$$\mathcal{C}_i:=\mathcal{C}_i(1+T):=\begin{pmatrix}a_p & 1\\ -\epsilon(p)\Phi_{p^i}(1+T) & 0\end{pmatrix}.$$

Definition 2.3. — We also put $C:=\begin{pmatrix}a_p & 1\\ -\epsilon(p)p & 0\end{pmatrix}$.

Definition 2.4. — We define the logarithm matrix $\mathcal{L}og_{\alpha,\beta}:=\mathcal{L}og_{\alpha,\beta}(1+T)$ by

$$\mathcal{L}og_{\alpha,\beta}(1+T):=\lim_{n\to\infty}\mathcal{C}_1\cdots\mathcal{C}_nC^{-(N+1)}\left(\begin{smallmatrix}-1 & -1\\ \beta & \alpha\end{smallmatrix}\right).$$

Convention 2.5. — Whenever we encounter an *expression* involving $\Phi_{p^i}(1{+}T)$, we let $\widehat{expression}$ be the corresponding expression involving $\widehat{\Phi}_{p^i}(1+T)$. For example, we let $\widehat{\mathcal{C}_i}$ be $\mathcal{C}_i$ with $-\epsilon(p)\widehat{\Phi}_{p^i}(1+T)$ in the lower left entry instead of $-\epsilon(p)\Phi_{p^i}(1+T)$, and

$$\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T) = \lim_{n\to\infty} \widehat{\mathcal{C}}_1 \cdots \widehat{\mathcal{C}}_n C^{-(N+1)} \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix}.$$

Observation 2.6. — For $n > i \geqslant 1$, we have $\widehat{\mathcal{C}}_i(\zeta_{p^n}) = \mathcal{C}_i(\zeta_{p^n}) = C$.

2.2. Convergence of the entries. —

Definition 2.7. — Recall that ord_p is the valuation on $\ _p$ normalized by $\mathrm{ord}_p(p) = 1$. Put

$$v = \mathrm{ord}_p(a_p).$$

Proposition 2.8. — *The entries in the left column of $\mathcal{L}og_{\alpha,\beta}(1+T)$ and $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ are well-defined and converge on the open unit disk when $v = 0$. When $v > 0$ or $T = \zeta_{p^n} - 1$ with $n \geqslant 0$, we can say the same about all four entries.*

Definition 2.9. — For a matrix $M = (m_{i,j})_{i,j}$ with entries $m_{i,j}$ in the domain of a valuation val, let the *valuation matrix* $[M]$ *of* M be the matrix consisting of the valuations of the entries:

$$[M] := [\mathrm{val}(m_{i,j})]_{i,j}.$$

Let $N = (n_{k,l})_{k,l}$ be another matrix so that we can form the product MN. Valuation matrices have the following (unnatural) *valuative multiplication* operation:

$$[M][N] := [\min_j(m_{i,j} + n_{j,k})]_{i,k}$$

We also define the *valuation* $\mathrm{val}(M)$ *of* M to be the minimum of the entries in the valuation matrix:

$$\mathrm{val}(M) := \min\{\mathrm{val}(m_{i,j})\}.$$

Definition 2.10. — Let $0 < r < 1$. For $f(T) \in {}_p[[T]]$ convergent on the open unit disk, we define its *valuation at* r to be

$$v_r(f(T)) := \inf_{|z|_p < r} \mathrm{ord}_p(f(z)).$$

We define the *valuation at* 0 to be

$$v_0(f(T)) := \mathrm{ord}_p(f(0)).$$

Lemma 2.11. — *Let* val *be a valuation, and M and N be matrices so that we can define their matrix product MN. Then* $\mathrm{val}(MN) \geqslant \mathrm{val}(M) + \mathrm{val}(N)$.

Proof. — Term by term, the entries of $[MN]$ are at least as big as those of $[M][N]$. *QED*

Notation 2.12. — Let M be a matrix whose coefficients are in $\ _p[[T]]$. With respect to v_r we may then define the *valuation matrix of* M *at* r and denote it by $[M]_r$. We similarly define the *valuation of* M *at* r and denote it by $v_r(M)$. When these terms don't depend on r (e.g. when the entries of M are constants), we drop the subscript r.

Example 2.13. — [(2)] *Denote the logarithm with base* p *by* $\log_{(p)}$ *to distinguish it from the* p*-adic logarithm* $\log_p$ *of Iwasawa.*

$$v_r\left(\Phi_{p^n}(1+T)\right) = \begin{cases} 1 & \textit{when } r \leqslant p^{-\frac{1}{p^{n-1}(p-1)}} \\ -\log_{(p)}(r)p^{n-1}(p-1) & \textit{when } r \geqslant p^{-\frac{1}{p^{n-1}(p-1)}} \end{cases}$$

Example 2.14. — $v_r\left((1+T)^{\frac{1}{2}p^{n-1}(p-1)}\right) = \frac{1}{2}p^{n-1}(p-1)v_r((1+T)) = 0.$

In what follows, we will give the necessary arguments needed for proving Proposition 2.8 for $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$. From the above Example 2.14, the proof for $\mathcal{L}og_{\alpha,\beta}(1+T)$ follows by taking the hat off the relevant expressions. Note that it suffices to prove the proposition for the matrix $\lim\limits_{n\to\infty} \widehat{\mathcal{C}}_1 \cdots \widehat{\mathcal{C}}_n C^{-n}$.

Lemma 2.15. — *Let* $0 \leqslant r < 1$. *For* $i \gg 0$, $\left[\widehat{\mathcal{C}}_i\right]_r = \left[\begin{smallmatrix} v & 0 \\ 1 & \infty \end{smallmatrix}\right] = [C]$.

Proof. — This follows from Example 2.13. *QED*

Lemma 2.16. — *Let* $n \geqslant 0$. *Then for* $i \gg 0$, *we have* $v_r\left(\widehat{\mathcal{C}}_{i+1} \cdots \widehat{\mathcal{C}}_{i+n}\right) \geqslant v_r(C^n)$.

Proof. — This is a consequence of the preceding Lemma 2.15 and the triangle inequality. *QED*

The next lemma gives the valuation matrices of positive powers of C.

Lemma 2.17. — *Let* $n > 1$ *be a positive integer. We have*

$$v_r(C^n) \geqslant \begin{cases} (n-1)v & \textit{if } v < \frac{1}{2}, \\ \frac{n-1}{2} & \textit{if } v \geqslant \frac{1}{2}. \end{cases}$$

$$v_r(C^{-n}) = v_r(C^n) - n \geqslant \frac{-n-1}{2} \textit{ if } v \geqslant \frac{1}{2}.$$

Proof. — When $v < \frac{1}{2}$, we have by induction

$$[C^n] = \left[\begin{smallmatrix} nv & (n-1)v \\ (n-1)v+1 & (n-2)v+1 \end{smallmatrix}\right].$$

When $v > \frac{1}{2}$, denote by "$\geqslant a$" an unspecified real number greater than or equal to a given real number a. Without loss of generality, let n be even. Then we find again by induction that

$$[C^n] = \left[\begin{smallmatrix} m & \geqslant v+m-1 \\ \geqslant v+m & m \end{smallmatrix}\right].$$

When $v = \frac{1}{2}$, we have

$$[C^n] = \left[\begin{smallmatrix} \geqslant m & \geqslant v+m-1 \\ \geqslant v+m & \geqslant m \end{smallmatrix}\right].$$

[(2)] This essentially appears in the proof of [**Po03**, lemma 4.5]. It seems that he meant to write $p^{-v_r(\Phi_n(1+T))} \sim r^{p^{n-1}(p-1)}$ in the proof.

QED

Lemma 2.18. — *Fix $0 \leqslant r < 1$. Then $v_r(\widehat{\mathcal{C}}_{n+1}C^{-1} - I) \geqslant n + c$ for $n \gg 0$, where c is a constant independent of n (which can be computed explicitly).*

Proof. — We prove the statement for $v_r\left(\mathcal{C}_{n+1}C^{-1} - I\right)$, which has the same arguments:

$$v_r\left(\mathcal{C}_{n+1}C^{-1} - I\right) = v_r\left(\frac{\Phi_{p^{n+1}}(1+T)}{p} - 1\right) = -v_r(p) + v_r\left(\left(\sum_{t\geqslant 0}^{t\leqslant p-1}(1+T)^{tp^n}\right) - p\right)$$

$$= -1 + v_r\left(\sum_{t\geqslant 1}^{t\leqslant p-1}\sum_{k\geqslant 1}^{k\leqslant tp^n}\left(\begin{array}{c} tp^n \\ k \end{array}\right)T^k\right) \geqslant -1 + \min_{\substack{1\leqslant t\leqslant p-1\\ 1\leqslant k\leqslant tp^n}} \operatorname{ord}_p\left(\begin{array}{c} tp^n \\ k \end{array}\right) + kv_r(T)$$

By [**Ku52**, discussion on page 116 after the Lehrsatz from page 115], this quantity is

$$\geqslant -1 + \min_{1\leqslant k\leqslant p^{n+1}-p^n}(n - \operatorname{ord}_p(k)) + kv_r(T).$$

Now note that $\min_{1\leqslant k\leqslant p^{n+1}-p^n}\Big(k(-\log_{(p)}(r)) - \operatorname{ord}_p(k)\Big)$ is of the form

$$p^m\Big(-\log_{(p)}(r)\Big) - m$$

for one constant m for all $n \gg 0$. *QED*

Proof of proposition. — Put

$$\widehat{V}_n := \widehat{\mathcal{C}}_1\cdots\widehat{\mathcal{C}}_n(\widehat{\mathcal{C}}_{n+1}C^{-1} - I).$$

By Lemma 2.11, we have

$$v_r(\widehat{V}_n) \geqslant v_r(\widehat{\mathcal{C}}_1\cdots\widehat{\mathcal{C}}_n) + v_r(\widehat{\mathcal{C}}_{n+1}C^{-1} - I).$$

We prove that as $n \to \infty$, the appropriate entries of the following matrix have arbitrarily large valuations:

$$\widehat{\mathcal{C}}_1\cdots\widehat{\mathcal{C}}_{n+1}C^{-(N+1)}\left(\begin{smallmatrix}-1 & -1\\ \beta & \alpha\end{smallmatrix}\right) - \widehat{\mathcal{C}}_1\cdots\widehat{\mathcal{C}}_nC^{-N}\left(\begin{smallmatrix}-1 & -1\\ \beta & \alpha\end{smallmatrix}\right)$$

$$= \begin{cases}\widehat{V}_n\left(\begin{smallmatrix}-1 & -1\\ \beta & \alpha\end{smallmatrix}\right)\left(\begin{smallmatrix}\alpha^{-N} & 0\\ 0 & \beta^{-N}\end{smallmatrix}\right), & \text{which we use for the case } v < \frac{1}{2},\\ \widehat{V}_nC^{-N}\left(\begin{smallmatrix}-1 & -1\\ \beta & \alpha\end{smallmatrix}\right), & \text{which comes in handy when } v \geqslant \frac{1}{2}.\end{cases}$$

For now, assume $v < \frac{1}{2}$. From Lemmas 2.16, 2.17, and 2.18 there are constants c, c' so that for $n \gg 0$,

$$v_r(\widehat{V}_n) + v_r\left(\begin{smallmatrix}-1 & -1\\ \beta & \alpha\end{smallmatrix}\right) + v_r(\alpha^{-N}) \geqslant (n-1)v + n + c - Nv \geqslant n + c'$$

and similarly,

$$v_r(\widehat{V}_n) + v_r\left(\begin{smallmatrix}-1 & -1\\ \beta & \alpha\end{smallmatrix}\right) + v_r(\beta^{-N}) \geqslant (n-1)v + n + c + N(v-1) \geqslant 2vn + c'.$$

For the case $v \geqslant \frac{1}{2}$, we have

$$v_r(\widehat{V}_nC^{-N}\left(\begin{smallmatrix}-1 & -1\\ \beta & \alpha\end{smallmatrix}\right)) \geqslant v_r(\widehat{\mathcal{C}}_1\cdots\widehat{\mathcal{C}}_n) + v_r(I - \widehat{\mathcal{C}}_{n+1}C^{-1}) + v_r(C^{-N}) + v_r\left(\begin{smallmatrix}-1 & -1\\ \beta & \alpha\end{smallmatrix}\right).$$

This quantity is $\geqslant \frac{n-1}{2} + n + c + \frac{-N-1}{2} \geqslant n + c'$ for constants c, c' independent of n.

Finally, when $T = \zeta_{p^n} - 1$, $\widehat{\mathcal{C}}_i(\zeta_{p^n}) = C$ for $i > n$, so $\widehat{\mathcal{L}og}_{\alpha,\beta}(\zeta_{p^n})$ is a finite product. *QED*

Remark 2.19 **(Nomenclator of the matrix $\mathcal{L}og_{\alpha,\beta}$).** — For odd p, we have:

$$\det \mathcal{L}og_{\alpha,\beta}(1+T) = \frac{\log_p(1+T)}{T} \times \frac{\beta - \alpha}{(\epsilon(p)p)^2}$$

For $p = 2$, the above exponent of 2 has to be replaced by a 3.

2.3. The rate of growth. —

Definition 2.20. — For $f(T), g(T) \in {}_p[[T]]$ converging on the open unit disc, we say $f(T)$ is $O(g(T))$ if

$$p^{-v_r(f(T))} \text{ is } O(p^{-v_r(g(T))}) \text{ as } r \to 1^-,$$

i.e. there is an $r_0 < 1$ and a constant C so that

$$v_r(g(T)) < v_r(f(T)) + C \text{ when } 1 > r > r_0.$$

If $g(T)$ is also $O(f(T))$, we say that "$f(T)$ grows like $g(T)$," and write $f(T) \sim g(T)$.

Example 2.21. — $1 \sim T \sim \Phi_p(1+T)$. *Also,* $\det \mathcal{L}og_{\alpha,\beta} \sim \log_p(1+T)$ *by Remark 2.19.*

Proposition 2.22 **(Growth Lemma).** — *The entries of* $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ *and* $\mathcal{L}og_{\alpha,\beta}(1+T)$ *grow like* $\log_p(1+T)^{\frac{1}{2}}$ *when* $v > \frac{1}{2}$. *When* $v \leqslant \frac{1}{2}$, *the entries in the left column are* $O(\log_p(1+T)^v)$. *When* $v = \frac{1}{2}$, *those of the right column are* $O(\log_p(1+T)^{1-v})$.

We give the proof for $\mathcal{L}og_{\alpha,\beta} = \mathcal{L}og_{\alpha,\beta}(1+T)$, since it is similar for the case $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$. Before beginning with the proof, let us name the quantities from Example 2.13:

Definition 2.23. — $e_{n,r} := v_r(\Phi_{p^n}(1+T)) = \min(1, -\log_{(p)}(r)(p^n - p^{n-1}))$

Also, diagonalization is very useful in the proof as well:

Observation 2.24. — Let m be an integer. Then $\begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix} \begin{pmatrix} \alpha^m & 0 \\ 0 & \beta^m \end{pmatrix} = C^m \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix}$.

Proof of Growth Lemma 2.22. — We first treat the case $v = 0 = \mathrm{ord}_p(\alpha)$. When $n \geqslant 1$,

$$[\mathcal{C}_1 \cdots \mathcal{C}_n]_r = [\mathcal{C}_1]_r \cdots [\mathcal{C}_n]_r = \begin{bmatrix} 0 & 0 \\ e_{1,r} & e_{1,r} \end{bmatrix}.$$

By Observation 2.24, the valuation matrix of the left column of $\mathcal{C}_1 \cdots \mathcal{C}_n \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix}$ and of $\mathcal{L}og_{\alpha,\beta}$ is $\begin{bmatrix} 0 \\ e_{1,r} \end{bmatrix}$. Thus, these entries are $O(\Phi_p(1+T))$. Since we have $\Phi_p(1+T) \sim 1$ by Example 2.21, they are indeed $O(1)$.

Next, we treat the case $v > \frac{1}{2}$. Without loss of generality, let $n > 1$ be even. Then

$$[\mathcal{C}_1 \cdots \mathcal{C}_n]_r = [\mathcal{C}_1]_r \cdots [\mathcal{C}_n]_r = \begin{bmatrix} e_{2,r} + e_{4,r} + \cdots + e_{n,r} & v + e_{1,r} + \cdots + e_{n-2,r} \\ v + e_{1,r} + \cdots + e_{n-1,r} & e_{1,r} + \cdots + e_{n-1,r} \end{bmatrix}.$$

From Observation 2.24, $\mathrm{ord}_p(\alpha) = \mathrm{ord}_p(\beta) = \frac{1}{2}$, and $e_{n,r} \leqslant 1$, we compute

$$\left[\mathcal{C}_1 \cdots \mathcal{C}_n C^{-(N+1)} \left(\begin{smallmatrix} -1 & -1 \\ \beta & \alpha \end{smallmatrix}\right)\right]_r = \left[\begin{array}{cc} -\frac{N}{2} + e_{2,r} + \cdots + e_{n,r} & -\frac{N}{2} + e_{2,r} + \cdots + e_{n,r} \\ \frac{1-N}{2} + e_{1,r} + \cdots + e_{n-1,r} & \frac{1-N}{2} + e_{1,r} + \cdots + e_{n-1,r} \end{array}\right].$$

These entries differ, by a constant independent from r, from

$$v_r\left(\prod_{k\geqslant 2, k \text{ even}}^{n} \frac{\Phi_{p^k}(1+T)}{p}\right) = e_{2,r} + \cdots + e_{n,r} - \frac{n}{2}, \text{ and}$$

$$v_r\left(\prod_{k\geqslant 1, k \text{ odd}}^{n} \frac{\Phi_{p^k}(1+T)}{p}\right) = e_{1,r} + \cdots + e_{n-1,r} - \frac{n}{2}.$$

But from [**Po03**, Lemma 4.5], we have

$$\prod_{\text{even } k\geqslant 2}^{\infty} \frac{\Phi_{p^k}(1+T)}{p} \sim \prod_{\text{odd } k\geqslant 1}^{\infty} \frac{\Phi_{p^k}(1+T)}{p} \sim \log_p(1+T)^{\frac{1}{2}},$$

from which the assertion of the lemma follows for the case $v > \frac{1}{2}$.

Lastly, we assume $0 < v \leqslant \frac{1}{2}$. Given r, let i be the largest integer so that $e_{i,r} < 2v$. Without loss of generality, assume i is even. We then compute

$$[\mathcal{C}_1 \cdots \mathcal{C}_i]_r = [\mathcal{C}_1]_r \cdots [\mathcal{C}_i]_r = \left[\begin{array}{cc} e_{2,r} + e_{4,r} + \cdots + e_{i,r} & v + e_{2,r} + \cdots + e_{i-2,r} \\ v + e_{1,r} + e_{3,r} + \cdots + e_{i-1,r} & e_{1,r} + \cdots + e_{i-1,r} \end{array}\right].$$

Remembering that $e_{i+1,r} \geqslant 2v$, we see that for $n > i$,

$$[\mathcal{C}_1 \cdots \mathcal{C}_n]_r = \left[\begin{array}{cc} (n-i)v + e_{2,r} + e_{4,r} + \cdots + e_{i,r} & (n-i-1)v + e_{2,r} + \cdots + e_{i,r} \\ \geqslant (n-i-1)v + e_{1,r} + \cdots + e_{i-1,r} & \geqslant (n-i)v + e_{1,r} + \cdots + e_{i-1,r} \end{array}\right],$$

where by $\geqslant x$ we have denoted an unspecified entry that is greater than or equal to x. By Observation 2.24, we have that $\left[\mathcal{C}_1 \cdots \mathcal{C}_n C^{-(N+1)} \left(\begin{smallmatrix} -1 & -1 \\ \beta & \alpha \end{smallmatrix}\right)\right]_r$ is

$$\left[\begin{array}{cc} \geqslant (n-N-i)v + e_{2,r} + \cdots + e_{i,r} & \geqslant (n+N-i)v - N + e_{2,r} + \cdots + e_{i,r} \\ \geqslant (n-N-i+1)v + e_{1,r} + \cdots + e_{i-1,r} & \geqslant (n+N-i+1)v - N + e_{1,r} + \cdots + e_{i-1,r} \end{array}\right].$$

Now let $m := i - \lfloor \mathrm{ord}_p(2v) \rfloor$. We then have $e_{m-h,r} \cdot 2v \leqslant e_{i-h,r}$ for any $h < i$, and $e_{M,r} = 1$ for any $M > m$. Thus, the top left entry of $\left[\mathcal{C}_1 \cdots \mathcal{C}_n C^{-(N+1)} \left(\begin{smallmatrix} -1 & -1 \\ \beta & \alpha \end{smallmatrix}\right)\right]_r$ is up to a constant independent from r greater than or equal to

$$2v(e_{m-i+2,r} + e_{m-i+4,r} + \cdots + e_{m,r}) - iv = 2v \cdot v_r\left(\prod_{k\geqslant m-i+2, k \text{ is even}}^{m} \frac{\Phi_{p^k}(1+T)}{p}\right).$$

The claim then follows from noting $\prod_{\text{even } k\geqslant 2}^{\infty} \frac{\Phi_{p^k}(1+T)}{p} \sim \log_p(1+T)^{\frac{1}{2}}$. Using similar arguments, one obtains the appropriate bound for the lower left entry, and for the right entries when $v = \frac{1}{2}$. *QED*

2.4. The functional equation. —

Proposition 2.25. — *Under the change* $(1+T) \mapsto (1+T)^{-1}$, *the first column of* $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ *is invariant.*

When all entries of $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ *converge, then:*
If p *is odd, then* $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T) = \widehat{\mathcal{L}og}_{\alpha,\beta}((1+T)^{-1})$.
If $p = 2$, *then* $\left(\begin{smallmatrix} 1 & 0 \\ 0 & (1+T)^{-1} \end{smallmatrix}\right) \widehat{\mathcal{L}og}_{\alpha,\beta}(1+T) = \widehat{\mathcal{L}og}_{\alpha,\beta}((1+T)^{-1})$.

Proof. — All $\widehat{\mathcal{C}}_i(1+T)$ are invariant under the change of variables $1+T \mapsto \frac{1}{1+T}$, except $\widehat{\mathcal{C}}_1(1+T)$ if $p = 2$, where we have $\widehat{\mathcal{C}}_1(\frac{1}{1+T}) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & (1+T)^{-1} \end{smallmatrix}\right) \widehat{\mathcal{C}}_1(1+T)$.

2.5. The functional equation in the case $a_p = 0$.— When $a_p = 0$, the entries of $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ are off by units from the corresponding ones in $\mathcal{L}og_{\alpha,\beta}(1+T)$. More precisely, denote by $\log_p^{\pm}(1+T)$ Pollack's half-logarithms [**Po03**]:

$$\log_p^+(T) := \frac{1}{p}\prod_{j\geqslant 1}\frac{\Phi_{p^{2j}}(1+T)}{p},$$

$$\log_p^-(T) := \frac{1}{p}\prod_{j\geqslant 1}\frac{\Phi_{p^{2j-1}}(1+T)}{p}.$$

We then have

$$\mathcal{L}og_{\alpha,\beta}(1+T) = \begin{cases} \frac{1}{\epsilon(p)}\left(\begin{smallmatrix} \log_p^+(T) & \log_p^+(T) \\ \log_p^-(T)\alpha & \log_p^-(T)\beta \end{smallmatrix}\right) & \text{when } p \text{ is odd,} \\ \frac{1}{\epsilon(2)}\left(\begin{smallmatrix} \frac{-1}{\epsilon(2)2}\log_2^+(T)\alpha & \frac{-1}{\epsilon(2)2}\log_2^+(T)\beta \\ \log_2^-(T) & \log_2^-(T) \end{smallmatrix}\right) & \text{when } p = 2. \end{cases}$$

Setting $U^{\pm}(1+T) := \widehat{\log_p^{\pm}(T)}/\log_p^{\pm}(T)$, we obtain

$$\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T) = \left(\begin{smallmatrix} U^+(1+T) & 0 \\ 0 & U^-(1+T) \end{smallmatrix}\right)\mathcal{L}og_{\alpha,\beta}(1+T).$$

Now put

$$W^+(1+T) = \frac{U^+(1+T)}{U^+((1+T)^{-1})} = \prod_{j\geqslant 1}(1+T)^{-p^{2j-1}(p-1)}, \text{ and}$$

$$W^-(1+T) = \begin{cases} \frac{U^-(1+T)}{U^-((1+T)^{-1})} = \prod_{j\geqslant 1}(1+T)^{-p^{2j-2}(p-1)} & \text{for odd } p, \\ \frac{U^-(1+T)}{(1+T)U^-((1+T)^{-1})} = (1+T)^{-1}\prod_{j\geqslant 2}(1+T)^{-p^{2j-2}(p-1)} & \text{when } p = 2. \end{cases}$$

We can finally arrive at the correct statement of [**Po03**, Lemma 4.6]:

Lemma 2.26. — *We have*

$$\log_p^+(T)W^+(1+T) = \log_p^+(\frac{1}{1+T}-1),$$

$$\log_p^-(T)W^-(1+T) = \log_p^-(\frac{1}{1+T}-1).$$

Proof. — This follows from what has been said above, or by going through the proof of [**Po03**, Lemma 4.6] on noting that the units $U^{\pm}(1+T) \neq 1$. *QED*

3. The two p-adic L-functions $\widehat{L}_p^\sharp(f,T)$ and $\widehat{L}_p^\flat(f,T)$

In this section, we construct Iwasawa functions $\widehat{L}_p^\sharp(f,T)$ and $\widehat{L}_p^\flat(f,T)$. We present the arguments with the completions. The corresponding non-completed arguments can be recovered by taking off the hat above any expression $\widehat{xyz}$ and replacing it by just xyz. Instead of working with the matrices $\widehat{\mathcal{C}}_i$ and C, we make our calculations easier via the following definitions:

Definition 3.1. —

$$\widehat{\mathcal{A}}_i := \begin{pmatrix} a_p & \widehat{\Phi}_{p^i}(1+T) \\ -\epsilon(p) & 0 \end{pmatrix}, A := \begin{pmatrix} a_p & p \\ -\epsilon(p) & 0 \end{pmatrix}, \tilde{A} := \begin{pmatrix} a_p & 1 \\ -\epsilon(p) & 0 \end{pmatrix}.$$

Definition 3.2. — For any integer i, put $Y_{2i} := p^{-i}A^{2i}$, and $Y_{2i+1} = Y_{2i}\tilde{A}$.

Proposition 3.3 **(Tandem Lemma).** — *Fix $n \in$. Assume that for any $i \in$, we are given functions $Q_i = Q_i(T)$ so that $Q_i \in \widehat{\Phi}_{p^i}(1+T)[T]$ whenever $i \leqslant n$, and $(Q_{n+1}, Q_n)Y_{n'-n} = (Q_{n'+1}, Q_{n'})$ for any $n' \in$. Then*

$$(Q_{n+1}, Q_n) = (\widetilde{q}_1, q_0)\widehat{\mathcal{A}}_1 \cdots \widehat{\mathcal{A}}_n \textit{ with } \widetilde{q}_1, q_0 \in [T].$$

Proof. — We inductively show that $(Q_{n+1}, Q_n) = (\widetilde{q}_{i+1}, q_i)\widehat{\mathcal{A}}_{i+1} \cdots \widehat{\mathcal{A}}_n$ for $\widetilde{q}_{i+1}, q_i \in [T]$ with $0 \leqslant i \leqslant n$: Note that at the base step $i = n$, the product of the $\widehat{\mathcal{A}}$'s is empty so that we indeed have $(\widetilde{q}_{n+1}, q_n) = (Q_{n+1}, Q_n)$. For the inductive step, let $i \geqslant 1$. Then we have

$$(Q_{n+1}, Q_n) = (\widetilde{q}_{i+1}, q_i)A^{n-i} \text{ by evaluation at } \zeta_{p^i} - 1, \text{ and}$$

$$(Q_{n+1}, Q_n)Y_{i-n} = (Q_{i+1}, Q_i) \text{ by assumption.}$$

We thus have $(\widetilde{q}_{i+1}, q_i)A^{n-i}Y_{i-n} = (Q_{i+1}, 0)$ at $\zeta_{p^i} - 1$, whence q_i vanishes at $\zeta_{p^i} - 1$. We hence write $q_i = \widehat{\Phi}_{p^i}(1+T) \cdot \widetilde{q}_i$ for some $\widetilde{q}_i \in [T]$. Now put $(\widetilde{q}_i, q_{i-1}) := (\widetilde{q}_{i+1}, \widetilde{q}_i)\tilde{A}^{-1}$. Then $(\widetilde{q}_{i+1}, q_i) = (\widetilde{q}_i, q_{i-1})\widehat{\mathcal{A}}_i$. *QED*

Observation 3.4. — Let $(\Theta_n)_n$ be a queue sequence and $\pi : \Lambda_n \to \Lambda_{n-1}$ be the projection. Then for $n \geqslant 2$, we have $\pi(\Theta_n, \nu\Theta_{n-1}) = (\Theta_{n-1}, \nu\Theta_{n-2})A$.

Proof. — Definition 1.6. *QED*

Proposition 3.5. — *Let $(\Theta_n)_n$ be a queue sequence and $1 \leqslant n' \leqslant n$. When identifying elements of Λ_n with their representatives in $[T]$, the second entry of $(\Theta_n, \nu\Theta_{n-1})Y_{n'-n}$ vanishes at $\zeta_{p^{n'}} - 1$.*

Proof. — Denote by $\pi_{n/n'}$ the projection from Λ_n to $\Lambda_{n'}$. By the above lemma, the second entry of

$$\pi_{n/n'}(\Theta_n, \nu\Theta_{n-1})Y_{n'-n} = (\Theta_{n'}, \nu\Theta_{n'-1})A^{n-n'}Y_{n'-n}$$

is contained in the ideal $(\Phi_{n'}) \subset \Lambda_{n'}$. Thus, its preimage under $\pi_{n/n'}$ is in the ideal $(\Phi_{n'}) \subset \Lambda_n$. *QED*

Corollary 3.6. — *Let $(\Theta_n)_n$ be a queue sequence. Then $(\Theta_n, \nu\Theta_{n-1}) = \widehat{\Upsilon}_n\widehat{\mathcal{C}}_1 \cdots \widehat{\mathcal{C}}_n\tilde{A}^{-1}$ for some $\widehat{\Upsilon}_n \in \Lambda_n^{\oplus 2}$.*

Proof. — We identify elements of Λ_n by their corresponding representative in $[T]$ and use Proposition 3.5. Then, we can apply the Tandem Lemma 3.3, and project back to $\Lambda_n^{\oplus 2}$. *QED*

Corollary 3.7. — *We can rewrite the Riemann sum approximations of Definition 1.9: For some* $\overrightarrow{\widehat{L_{p,n}^{\omega^i}}} \in [T]^{\oplus 2}$,

$$\begin{aligned}\left(\varepsilon_{\omega^i} L_{N,\alpha}^{sign(\omega^i)}, \varepsilon_{\omega^i} L_{N,\beta}^{sign(\omega^i)}\right) &= \overrightarrow{\widehat{L_{p,n}^{\omega^i}}} \widehat{\mathcal{C}}_1 \cdots \widehat{\mathcal{C}}_n \tilde{A}^{-1} \left(\begin{smallmatrix} \alpha^{-N} & \beta^{-N} \\ -\alpha^{-(N+1)} & -\beta^{-(N+1)} \end{smallmatrix}\right) \\ &= \overrightarrow{\widehat{L_{p,n}^{\omega^i}}} \widehat{\mathcal{C}}_1 \cdots \widehat{\mathcal{C}}_n C^{-(N+1)} \left(\begin{smallmatrix} -1 & -1 \\ \beta & \alpha \end{smallmatrix}\right).\end{aligned}$$

Proof. — We know that $(\alpha^{N+1} L_{N,\alpha}, \beta^{N+1} L_{N,\beta}) = (\vartheta_N, \nu\vartheta_{N-1}) \left(\begin{smallmatrix} \alpha & \beta \\ -\epsilon & -\epsilon \end{smallmatrix}\right)$. The isotypical components of ϑ_N form queue sequences, so we can apply the above Corollary 3.6. *QED*

Taking limits, we obtain that

$$\lim_{n \to \infty} \overrightarrow{\widehat{L_{p,n}^{\omega^i}}} = \left(\widehat{L}_p^\sharp(f, \omega^i, T), \widehat{L}_p^\flat(f, \omega^i, T)\right) \in \Lambda^{\oplus 2}.$$

Applying Proposition 2.8, we obtain Theorem 1.13. When the objects involved come from the trivial character $ = \omega^0$, we drop their dependence on it in the notation, and Theorem 1.13 becomes:

Theorem 3.8. — *We have*

$$(L_p(f,\alpha,T), L_p(f,\beta,T)) = \begin{cases} \left(\widehat{L}_p^\sharp(f,T), \widehat{L}_p^\flat(f,T)\right) \widehat{\mathcal{L}og}_{\alpha,\beta}(1+T) \\ \left(L_p^\sharp(f,T), L_p^\flat(f,T)\right) \mathcal{L}og_{\alpha,\beta}(1+T) \end{cases} \quad \textit{for supersingular } p,$$

$$L_p(f,\alpha,T) = \begin{cases} \left(\widehat{L}_p^\sharp(f,T), \widehat{L}_p^\flat(f,T)\right) \left(\begin{smallmatrix} \widehat{\log}_\alpha^\sharp(1+T) \\ \widehat{\log}_\alpha^\flat(1+T) \end{smallmatrix}\right) \\ \left(L_p^\sharp(f,T), L_p^\flat(f,T)\right) \left(\begin{smallmatrix} \log_\alpha^\sharp(1+T) \\ \log_\alpha^\flat(1+T) \end{smallmatrix}\right) \end{cases} \quad \textit{for ordinary } p,$$

where $\left(\begin{smallmatrix} \widehat{\log}_\alpha^\sharp(1+T) \\ \widehat{\log}_\alpha^\flat(1+T) \end{smallmatrix}\right)$ *and* $\left(\begin{smallmatrix} \log_\alpha^\sharp(1+T) \\ \log_\alpha^\flat(1+T) \end{smallmatrix}\right)$ *are the first columns of* $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ *and* $\mathcal{L}og_{\alpha,\beta}(1+T)$.

Remark 3.9. — In our setup so far, we have worked with the periods $\Omega_f^\pm$. In the case of an elliptic curve E over $\mathbb{Q}$, one can alternatively use the real and imaginary Néron periods $\Omega_E^\pm$. These real and imaginary Néron periods are defined as follows:

Definition 3.10. — Decompose $H_1(E,) = H_1(E,)^+ \oplus H_1(E,)^-$, where complex conjugation acts as $+1$ on the first summand and as -1 on the second. Choose generators $\delta^\pm$ of $H_1(E,)^\pm$ so that the following integrals are positive:

$$\Omega_E^\pm := \begin{cases} \int_{\delta^\pm} \omega_E & \text{if } E() \text{ is connected,} \\ 2 \cdot \int_{\delta^\pm} \omega_E & \text{if not.} \end{cases}$$

We designate the corresponding modular symbols and p-adic L-functions by replacing f by E. In view of **[BCDT]** and **[Wi95]**, we have a modular parametrization $\pi : X_0(N) \to E$, so that $\pi^*(\omega_E) = c \cdot f_E \cdot \frac{dq}{q}$ for some normalized weight two newform f_E of level N. The constant

c is called the **Manin constant** for π. It is known to be an integer (cf. [**Ed91**, Proposition 2]) and conjectured to be 1. See [**Ma72**, § 5].

We note that the analogue of Theorem 1.1 is not necessarily satisfied when one replaces $\Omega_f^\pm$ by $\Omega_E^\pm$, but the following is known (cf. [**Po03**, Remark 5.4, Remark 5.5]):

Theorem 3.11 **(Imitation of Theorem 1.1)**. — *Let E be an elliptic curve over $\mathbb{Q}$, and p be a prime of good reduction. Then:*

1. [**AU96**, Théorème A] *p does not divide c.*
2. [**Ma72**, Theorem 3.3] *If $a_p \not\equiv 1 \mod p$, we have $2\left[\frac{a}{p^n}\right]_E^\pm \in c^{-1}$, so $2\left[\frac{a}{p^n}\right]_E^\pm \in \;{}_p$.*

Corollary 3.12. — *When $a_p \not\equiv 1 \mod p$, $L_p^\sharp(E,\omega^i,T)$ and $L_p^\flat(E,\omega^i,T)$ and their completions are in Λ. In particular, the 2-adic L-functions $L_2^\sharp(E,\omega^i,T)$ and $L_2^\flat(E,\omega^i,T)$ from* [**Sp12**, Definition 6.1] *agree with those of this paper and are consequently elements of Λ.*

Proof. — This follows from Theorem 1.13 and what has just been said. For $p=2$, we exploit the following symmetry in the isotypical components of the Riemann sums $L_{N,\alpha}^\pm$ and $L_{N,\beta}^\pm$: From $\eta^\pm(\frac{a}{m}) = \pm\eta^\pm(\frac{-a}{m})$, we can conclude that $\omega^i(a)\eta^\pm(\frac{a}{m}) = \pm\omega^i(-a)\eta^\pm(\frac{-a}{m})$. *QED*

Corollary 3.13 **(Analogue of Theorem 1.13)**. — *When $a_p \not\equiv 1 \mod p$, the statement of Theorem 1.13 with f formally replaced by E is still valid. When $a_p \equiv 1 \mod p$, we can say the same with the added caveat that $L_p^\sharp(E,\omega^i,T)$, $L_p^\flat(E,\omega^i,T)$, and their completions are elements of $\mathbb{Q}\otimes\Lambda$.*

Right from the definitions, we can also extract the following corollary, whose assumptions are satisfied when p is supersingular and $T \neq \zeta_{p^n}-1$ for any $n \geqslant 1$.

Corollary 3.14. — *Choose T so that $\mathcal{L}og_{\alpha,\beta}(1+T)$ converges and $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ is invertible. Then*

$$(\widehat{L}_p^\sharp(f,T),\widehat{L}_p^\flat(f,T)) = (L_p^\sharp(f,T),L_p^\flat(f,T))\mathcal{L}og_{\alpha,\beta}(1+T)\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)^{-1}.$$

From Theorem 1.5, we can give a table of the special values for a good prime p:

	$L_p^\sharp\left(f,\omega^i,0\right)$	$L_p^\flat\left(f,\omega^i,0\right)$
p odd, $i=0$	$\left(-a_p^2+2a_p+p-1\right)\frac{L(f,1)}{\Omega_f^+}$	$(2-a_p)\frac{L(f,1)}{\Omega_f^+}$
p odd, $i\neq 0$	$-pa_p\frac{L\left(f,\omega^{-i},1\right)}{\tau(\omega^{-i})\Omega_f^{\omega^i(-1)}}$	$-p\frac{L\left(f,\omega^{-i},1\right)}{\tau(\omega^{-i})\Omega_f^{\omega^i(-1)}}$
$p=2$, $i=0$	$\left(-a_p^3+2a_p^2+2pa_p-a_p-2p\right)\frac{L(f,1)}{\Omega_f^+}$	$\left(-a_p^2+2a_p+p-1\right)\frac{L(f,1)}{\Omega_f^+}$
$p=2$, $i\neq 0$	$-p^2a_p\frac{L\left(f,\omega^{-i},1\right)}{\tau(\omega^{-i})\Omega_f^{\omega^i(-1)}}$	$-p^2\frac{L\left(f,\omega^{-i},1\right)}{\tau(\omega^{-i})\Omega_f^{\omega^i(-1)}}$

In view of these special values, it seems reasonable to make the following conjecture:

Conjecture 3.15. — *Let f be a modular form as above, and let p be a good prime.*

When p is odd, the p-adic L-function $\widehat{L}_p^\flat(f,T)$ and $L_p^\flat(f,T)$ are not identically zero and $\widehat{L}_p^\sharp(f,T)$ and $L_p^\sharp(f,T)$ are not identically zero when $a_p \neq 2$. When $p=2$, the power series $\widehat{L}_2^\sharp(f,T)$ and $L_2^\sharp(f,T)$ are not identically zero and $\widehat{L}_2^\flat(f,T)$ and $L_2^\flat(f,T)$ are not identically zero when $a_2 \neq 1$.

3.1. Functional Equation. — Recall that f is a weight two modular form of level N and nebentype ϵ which is an eigenform for all T_n. Recall also Definition 1.7 of $\log_\gamma(\cdot)$. We denote by $f^* = w_N(f) = \epsilon(-1)f$ the involuted form of f under the Atkin-Lehner/Fricke operator, as in [**MTT**, (5.1)], and let $\alpha^* = \frac{\alpha}{\epsilon(p)}$ and $\beta^* = \frac{\beta}{\epsilon(p)}$.

Theorem 3.16. — *Let p be a prime so that $(p,N)=1$, i.e. $N \in {}^{\times}_{p} \cong \mathcal{G}_\infty$. When $\epsilon(p)=1$, $\widehat{L}_p^\sharp(f,\omega^i,T)$ and $\widehat{L}_p^\flat(f,\omega^i,T)$ satisfy the following functional equation:*

$$\widehat{L}_p^\sharp(f,\omega^i,T) = -\epsilon(-1)(1+T)^{-\log_\gamma(N)}\omega^i(-N)\widehat{L}_p^\sharp(f,\omega^i,\tfrac{1}{1+T}-1), \text{ and}$$
$$\widehat{L}_p^\flat(f,\omega^i,T) = -\epsilon(-1)(1+T)^{-\log_\gamma(N)}\omega^i(-N)\widehat{L}_p^\flat(f,\omega^i,\tfrac{1}{1+T}-1).$$

For general $\epsilon(p)$, let T be so that $\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T)$ and $\widehat{\mathcal{L}og}_{\alpha^*,\beta^*}(1+T)$ converge. Then

$$\left(\widehat{L}_p^\sharp(f,\omega^i,T),\widehat{L}_p^\flat(f,\omega^i,T)\right)\widehat{\mathcal{L}og}_{\alpha,\beta}(1+T) =$$
$$-\epsilon(-1)(1+T)^{-\log_\gamma(N)}\omega^i(-N)\left(\widehat{L}_p^\sharp(f^*,\omega^i,\tfrac{1}{1+T}-1),\widehat{L}_p^\flat(f^*,\omega^i,\tfrac{1}{1+T}-1)\right)\widehat{\mathcal{L}og}_{\alpha^*,\beta^*}(1+T).$$

Corollary 3.17. — *For an elliptic curve E over $\mathbb{Q}$ and a good prime p, we have*

$$\widehat{L}_p^\sharp(E,\omega^i,T) = -\epsilon(-1)(1+T)^{-\log_\gamma(N)}\omega^i(-N)\widehat{L}_p^\sharp(E,\omega^i,\tfrac{1}{1+T}-1), \text{ and}$$
$$\widehat{L}_p^\flat(E,\omega^i,T) = -\epsilon(-1)(1+T)^{-\log_\gamma(N)}\omega^i(-N)\widehat{L}_p^\flat(E,\omega^i,\tfrac{1}{1+T}-1).$$

When $a_p=0$, we can give an explicit functional equation for the non-completed p-adic L-functions, which corrects [**Po03**, Theorem 5.13] *in the case $i=0$:*

$$L_p^\sharp(E,\omega^i,T) = -\epsilon(-1)(1+T)^{-\log_\gamma(N)}\omega^i(-N)W^+(1+T)L_p^\sharp(E,\omega^i,\tfrac{1}{1+T}-1), \text{ and}$$
$$L_p^\flat(E,\omega^i,T) = -\epsilon(-1)(1+T)^{-\log_\gamma(N)}\omega^i(-N)W^-(1+T)L_p^\flat(E,\omega^i,\tfrac{1}{1+T}-1).$$

Proof of Theorem 3.16. — From [**MTT**, Proposition in §I.6], we have

$$\left[\frac{a}{p^n}\right]_f^\pm = -\epsilon(-p^n)\left[\frac{a'}{p^n}\right]_{f^*}^\pm = \epsilon(p^n)\left[\frac{a'}{p^n}\right]_f^\pm,$$

where $a' \in (\;/p^n\;)^*$ is chosen so that $a' \equiv \frac{-1}{Na} \bmod p^n$ (which explains the "root numbers" in the functional equation). Following through the substitution $a \mapsto a'$ gives us a functional equation for the Mazur-Tate symbols. In view of Corollary 3.7, the invariance of $\widehat{\mathcal{C}}_i(1+T)$ under $(1+T) \mapsto (1+T)^{-1}$ then gives the functional equation away from $T = \zeta_{p^n}-1$ for $n \geqslant 1$. To include those points, we use continuity. *QED*

4. A conjecture by Greenberg

Let p a good supersingular prime for an elliptic curve. Greenberg conjectured in [**Gr01**] that $L_p(E,\alpha,T)$ and $L_p(E,\beta,T)$ have finitely many common zeros. We now prove this for weight two modular forms.

Theorem 4.1. — *(Rohrlich) $L_p(f,\alpha,\omega^i,T)$ and $L_p(f,\beta,\omega^i,T)$ each vanish at finitely many $T=\zeta_{p^n}-1$.*

Proof. — By interpolation (Theorem 1.5), this follows from his original theorem [**Ro84**], which guarantees that $L(f,\chi,1)=0$ at finitely many characters of p-power order. *QED*

Theorem 4.2. — *$L_p(f,\alpha,\omega^i,T)$ and $L_p(f,\beta,\omega^i,T)$ have finitely many common zeros. In particular, so do $L_p(E,\alpha,T)$ and $L_p(E,\beta,T)$.*

Proof. — When a zero is not a p-power root of unity, it is one of the finitely many zeros of $L_p^\sharp(f,\omega^i,T)$ and $L_p^\flat(f,\omega^i,T)$, since $\det\mathcal{L}og_{\alpha,\beta}(1+T)$ doesn't vanish there. For the other zeros, use Rohrlich's theorem. *QED*

Remark 4.3. — Pollack has found a proof for this theorem in the case $a_p=0$ ([**Po03**, Corollary 5.12]).

5. The p-adic versions of the conjectures of Birch and Swinnerton-Dyer

We now unify the p-adic versions of the conjectures of Birch and Swinnerton-Dyer of Mazur, Tate, and Teitelbaum (for the ordinary case) and of Bernardi and Perrin-Riou (for the supersingular case) in terms of the vector of p-adic L-functions $(L_p^\sharp(E,T),L_p^\flat(E,T))$. We then pose a stronger conjecture concerning $L_p^\sharp(E,T)$ and $L_p^\flat(E,T)$ *individually.* This can also be done with $\widehat{L}_p^\sharp(E,T)$ and $\widehat{L}_p^\flat(E,T)$, cf. Remark 5.29.

5.1. Dieudonné modules and p-adic heights.

— The Dieudonné module is the following two-dimensional $\mathbb{Q}_p$-vector space:

$$D_p(E):=\mathbb{Q}_p\otimes H^1_{dR}(E/\mathbb{Q})$$

There is a Frobenius endomorphism φ which acts on $D_p(E)$ linearly. We refer the reader to [**BPR**, Paragraph 2] for a concrete definition, but let us record that its characteristic polynomial is $X^2-\frac{a_p}{p}X+\frac{1}{p}$, as opposed to the definition of [**MST**] or [**Ke01**] (where it is X^2-a_pX+p). This vector space admits a basis ω and $\varphi(\omega)$, where ω is the invariant/Néron differential of E. We now define eigenvectors $\nu_A:=\nu_{\frac{1}{\alpha}}$ and $\nu_B:=\nu_{\frac{1}{\beta}}$ of φ with eigenvalues $\frac{1}{\alpha}$ and $\frac{1}{\beta}$ which live in the $\mathbb{Q}_p(\alpha)$-vector space

$$D_p(E)(\alpha):=\mathbb{Q}_p(\alpha)\otimes H^1_{dR}(E/\mathbb{Q}).$$

Definition 5.1. — We define both eigenvectors as components of a vector:

$$\begin{pmatrix} \nu_A \\ \nu_B \end{pmatrix} := \begin{pmatrix} -\alpha & p \\ \beta & -p \end{pmatrix} \frac{1}{\beta-\alpha} \begin{pmatrix} \omega \\ \varphi(\omega) \end{pmatrix}$$

Definition 5.2. — When p is supersingular, Perrin-Riou's p-adic L-function can be defined via the classical p-adic L-functions $L_\alpha := L_\alpha(E,\alpha,T)$ and $L_\beta := L_p(E,\beta,T)$:

$$L_p^{PR}(E,T) := (L_\alpha, L_\beta) \begin{pmatrix} \nu_A \\ \nu_B \end{pmatrix}$$

This is equivalent via the arguments in [**SW**, Section 3.5] to Perrin-Riou's construction in [**PR03**, Section 2.2].

***Lemma 5.3* ($D_p(E)$-rationality of coefficients).** — *We have* $L_p^{PR}(E,T) \in D_p(E)[[T]]$.

Proof. — By Theorem 1.13, we can write

$$L_p^{PR}(E,T) = (L_p^\sharp, L_p^\flat)\mathcal{L}og_{\alpha,\beta} \left(\begin{smallmatrix} 1 & \alpha \\ 1 & \beta \end{smallmatrix}\right)^{-1} \left(\begin{smallmatrix} 1 & 0 \\ a_p & -p \end{smallmatrix}\right) \left(\begin{smallmatrix} \omega \\ \varphi(\omega) \end{smallmatrix}\right).$$

From the definition of $\mathcal{L}og_{\alpha,\beta}$, we then see that $L_p^{PR}(E,T) \in D_p(E)[[T]]$, as desired. *QED*

Given a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for E, recall that the associated Néron/invariant differential is $\omega = \frac{dx}{2y+a_1x+a_3}$ (see e.g. [**Si09**, Chapter III.1]. The $\mathbb{Q}$-vector space $H^1_{dR}(E/\mathbb{Q})$ admits a basis $\{\omega, x\omega\}$ and is equipped with a canonical alternating bilinear form $[\cdot,\cdot]$ so that $[\omega, x\omega] = 1$. We extend it linearly to the Dieudonné modules above and denote these extensions by $[\cdot,\cdot]$ as well.

Fix ω. Then for each $\nu \in D_p(E)$ (resp. $\nu \in D_p(E)(\alpha)$), one can associate a quadratic form h_ν mapping from $E(\mathbb{Q})$ to $\mathbb{Q}_p$ (resp. to $\mathbb{Q}_p(\alpha)$). One can do this (see [**BPR**], or [**SW**]) by defining preliminary height functions h'_ω and $h'_{x\omega}$, and then extending linearly, i.e. given $\nu = a\omega + bx\omega$, let $h'_\nu = ah'_\omega + bh'_{x\omega}$. Explicitly, we have $h'_\omega(P) = -\log_\omega(P)^2$, where $\log_\omega$ is the logarithm associated to ω. The definition of $h'_{x\omega}$ involves the σ-functions of either Mazur and Tate or of Bernardi. We refer to [**SW**, Section 4] for an explicit definition, since it won't be needed in this paper. We then put $h_\nu := \frac{h'_\nu}{\log_p(\gamma)}$.

Remark 5.4. — The reason for this normalization is that classically, p-adic L-functions $L_p(T)$ are thought of as functions of a variable s via the substitution $T = \gamma^{s-1} - 1$, cf. [**MTT**, §II.13]. The original formulation of p-adic BSD then investigated the behavior of a particular $L_p(\gamma^{s-1}-1)$ at $s = 1$. Note that

$$\frac{d^r}{ds^r} L_p(\gamma^{s-1}-1)|_{s=1} = \frac{d^r}{dT^r} L_p(T)\bigg|_{T=0} \cdot \log_p(\gamma)^r.$$

From this height function, we now assemble the following bilinear form with values in $\mathbb{Q}_p$ (resp.$\mathbb{Q}_p(\alpha)$):

$$\langle P, Q\rangle_\nu = \frac{1}{2}\left(h_\nu(P+Q) - h_\nu(P) - h_\nu(Q)\right)$$

Definition 5.5. — Let Reg_ν be the discriminant of this height pairing on $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$.

Definition 5.6. — Let ν_A and ν_B be as above. We define two normalized height functions

$$\hat{h}_{\nu_A} := \frac{h_{\nu_A}}{[\nu_B, \nu_A]} = \frac{h_{\nu_A}}{[\omega, \nu_A]} \text{ and } \hat{h}_{\nu_B} := \frac{h_{\nu_B}}{[\nu_A, \nu_B]} = \frac{h_{\nu_B}}{[\omega, \nu_B]},$$

and denote their corresponding regulators by $\mathrm{Reg}_{\frac{1}{\alpha}}$ and $\mathrm{Reg}_{\frac{1}{\beta}}$. Note that they are independent from the choice of our Weierstraß equation.

Denote by $r(E)$ the rank of $E(\mathbb{Q})$. In the supersingular case, Perrin-Riou defines the regulator $\mathrm{Reg}_p^{BPR}(E/\mathbb{Q})$ as the unique element in $D_p(E)$ so that for any $\nu \in D_p(E)$ so that $\nu \notin \mathbb{Q}_p\omega$, we have [(3)]

$$\left[\mathrm{Reg}_p^{BPR}(E/\mathbb{Q}), \nu\right] = \frac{\mathrm{Reg}_\nu}{[\omega, \nu]^{r-1}} \text{ where } r = r(E) > 0. \tag{1}$$

For $r(E) = 0$, she puts $\mathrm{Reg}_p^{BPR}(E/\mathbb{Q}) = \omega$.

Definition 5.7. — Let $r = r(E)$. Given a vector $\nu \in D_p(E)$ (or in $D_p(E)(\alpha)$) that is not a linear multiple of ω, we put

$$\widetilde{\mathrm{Reg}_\nu} := \frac{\mathrm{Reg}_\nu}{[\omega, \nu]^{r-1}}.$$

Remark 5.8. — We know that $\widetilde{\mathrm{Reg}_\nu}$ is linear in ν. See e.g. [**SW**, proof of Lemma 4.2].

Definition 5.9. — As an element of $D_p(E)(\alpha)$, define

$$\mathrm{Reg}_p(E/\mathbb{Q}) := (\mathrm{Reg}_{\frac{1}{\beta}}, \mathrm{Reg}_{\frac{1}{\alpha}}) \begin{pmatrix} \nu_A \\ \nu_B \end{pmatrix}.$$

Proposition 5.10. — *We have* $\mathrm{Reg}_p(E/\mathbb{Q}) \in D_p(E)$*, and when* p *is supersingular,* $\mathrm{Reg}_p(E/\mathbb{Q}) = \mathrm{Reg}_p^{BPR}(E/\mathbb{Q})$.

Proof. — When p is ordinary, we have $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p$, so there is nothing to prove. In the supersingular case, we only have to prove that $\mathrm{Reg}_p(E/\mathbb{Q}) = \mathrm{Reg}_p^{BPR}(E/\mathbb{Q})$:

When $r(E) = 0$, this follows from the fact that $\mathrm{Reg}_{\frac{1}{\alpha}} = 1$ and $\mathrm{Reg}_{\frac{1}{\beta}} = 1$.

When $r(E) > 0$, note that

$$\left[\mathrm{Reg}_p(E/\mathbb{Q}), \nu_A\right] = \mathrm{Reg}_{\frac{1}{\alpha}} \cdot [\nu_B, \nu_A] = \frac{\mathrm{Reg}_{\nu_A}}{[\nu_B, \nu_A]^{r-1}} = \frac{\mathrm{Reg}_{\nu_A}}{[\omega, \nu_A]^{r-1}},$$

and similarly, $\left[\mathrm{Reg}_p(E/\mathbb{Q}), \nu_B\right] = \frac{\mathrm{Reg}_{\nu_B}}{[\omega, \nu_B]^{r-1}}$. Since ν_A and ν_B form a basis for $D_p(E)(\alpha)$, linearity tells us that the property described in equation (1) holds for any $\nu \in D_p(E)(\alpha)$.

[(3)] This characterization is that of [**SW**, Lemma 4.2], which is a corrected version of Perrin-Riou's original lemma, [**PR03**, Lemme 2.6].

Now suppose that $\Delta := \mathrm{Reg}_p(E/\mathbb{Q}) - \mathrm{Reg}_p^{BPR}(E/\mathbb{Q}) \neq 0$. Then

$$[\Delta, \nu] = 0 \text{ for any } \nu \in D_p(E),$$

so this would in particular hold for $\nu = \omega$ or $\nu = x\omega$, from which we conclude by linearity that

$$[\Delta, \nu] = 0 \text{ for any } \nu \in D_p(E)(\alpha).$$

But then $\Delta = 0$, Q.E.A. *QED*

5.2. Statement of the conjectures. — We first recall the classical conjectures of Birch and Swinnerton-Dyer. Denote by $\omega = \omega_E$ the Néron differential and by $\Omega_E = \int_{E(\mathbb{R})} \omega \in \ {}^{>0}$ the Néron period of E. Note that we have $\Omega_E^+ = \Omega_E$ when $E(\ \ )$ is connected. If not, we have $\Omega_E^+ = \frac{\Omega_E}{2}$. Here, Ω_E^+ is the *real* Néron period from Definition 3.10. We write $r_{\mathbb{C}}$ for the order of vanishing of the Hasse-Weil L-function $L(E,s)$ at 1. We also let $r(E)$ be the rank of $E(\mathbb{Q})$, and denote by $L^*(E)$ the leading coefficient of the Taylor expansion at $s = 1$.

Conjecture 5.11 **(Birch and Swinnerton-Dyer).** — *The classical conjectures:*

1. *We have* $r_{\mathbb{C}} = r(E)$.
2. $\frac{L^*(E)}{\Omega_E} = \frac{\prod_v c_v \cdot \#Ш(E/\mathbb{Q}) \cdot \mathrm{Reg}_{\mathbb{C}}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tors})^2}$.

Here, c_v denotes the Tamagawa number for a place v, the regulator $\mathrm{Reg}_{\mathbb{C}}(E/\mathbb{Q})$ *is the discriminant of the Néron-Tate canonical height pairing on $E(\mathbb{Q})$, and $E(\mathbb{Q})_{tors}$ designates the torsion points of $E(\mathbb{Q})$.*

There are two p-adic analogues of this conjecture when p has good reduction:

Conjecture 5.12 **(Mazur, Tate, and Teitelbaum).** — *Let p be a good ordinary prime, and denote by r_p the order of vanishing of $L_p(E, \alpha, T)$ at 0, and by $L_p^*(E)$ the leading coefficient of the Taylor expansion at 0.*

1. *We have* $r_p = r(E)$.
2. $L_p^*(E) = \left(1 - \frac{1}{\alpha}\right)^2 \frac{\prod_v c_v \cdot \#Ш(E/\mathbb{Q}) \cdot \mathrm{Reg}_{\frac{1}{\beta}}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tors})^2}$.

Remark 5.13. — These conjectures are a combination of [**MTT**, §II.10, Conjecture (BSD(p))], which asserts that $r_p \geqslant r(E)$, and the remark thereafter, which predicts the non-vanishing of $\mathrm{Reg}_{\frac{1}{\beta}}(E/\mathbb{Q})$.

Remark 5.14. — We encounter the term $\mathrm{Reg}_{\frac{1}{\beta}}$ (rather than $\mathrm{Reg}_{\frac{1}{\alpha}}$) because of our choice of Frobenius $\varphi = \frac{F}{p}$, where F is the Frobenius as chosen in [**MST**] or [**Ke01**]. The regulator comes from the normalized height associated to the unit-eigenvector α of F on $D_p(E)$, so that the eigenvalue for φ becomes $\frac{\alpha}{p} = \frac{1}{\beta}$.[4]

[4] In [**SW**, Section 4.1], the regulator was accidentally constructed from the height coming from the normalized eigenvector of φ with eigenvalue $\frac{1}{\alpha}$. Everything works in that section if one replaces α by β.

Remark 5.15. — There are two constructions due to Kato and Perrin-Riou, cf. [**LZ**], and Pollack and Stevens [**PoSt**] of the critical slope p-adic L-function associated to the root β. Since we can evaluate the vector $(L_p^\sharp(E,T), L_p^\flat(E,T))\mathcal{L}og_{\alpha,\beta}(1+T)$ at $T=0$, it seems that there should also be a version of BSD involving this critical p-adic L-function and the formula for the residue should be the same as above with α and β interchanged.

For supersingular p, we have (cf. [**BPR**, Conjecture on page 229] and [**PR03**, Conjecture 2.5]):

Conjecture 5.16 **(Bernardi and Perrin-Riou).** — *Let p be a good supersingular prime, and denote by r_p the order of vanishing of $L_p^{PR}(E,T)$ at 0, and by $L_p^{PR*}(E)$ its leading coefficient (with value in the Dieudonné module) of its Taylor expansion around* 0.

1. *We have $r_p = r(E)$.*
2. $L_p^{PR*}(E) = (1-\varphi)^2 \frac{\prod_v c_v \cdot \# Ш(E/\mathbb{Q})}{(\# E(\mathbb{Q})_{tors})^2} \mathrm{Reg}_p(E/\mathbb{Q})$.

Remark 5.17. — Note that while the objects in the second part of this conjecture depend on the choice of Weierstraß equation, their coordinates with respect to the basis $\{\nu_\alpha, \nu_\beta\}$ don't. In fact, one can formulate Bernardi's and Perrin-Riou's conjecture in a form that resembles more closely that of the one given by Mazur, Tate, and Teitelbaum:

Conjecture 5.18 **(Equivalent formulation of above).** — *Let r_p the order of vanishing of L_α and L_β, and L_α^* and L_β^* the leading coefficients in the Taylor expansion. Then*

1. $r_p = r(E)$.
2. $L_\alpha^* = (1-\frac{1}{\alpha})^2 \frac{\prod_v c_v \cdot \# Ш(E/\mathbb{Q}) \cdot \mathrm{Reg}_{\frac{1}{\beta}}}{(\# E(\mathbb{Q})_{tors})^2}$, *and* $L_\beta^* = (1-\frac{1}{\beta})^2 \frac{\prod_v c_v \cdot \# Ш(E/\mathbb{Q}) \cdot \mathrm{Reg}_{\frac{1}{\alpha}}}{(\# E(\mathbb{Q})_{tors})^2}$.

This version can be found in [**Co04**, Conjecture 0.12], where it is attributed to Mazur, Tate and Teitelbaum.

5.3. A version of the conjectures via $L_p^\sharp$ and $L_p^\flat$.

— We now formulate a p-adic version of the conjecture of Birch and Swinnerton-Dyer using our pair of p-adic L-functions. As suggested by the title of this subsection, we drop the dependence on E and the variable T to simplify notation.

Definition 5.19. — We call $\overrightarrow{L}_p(E,T) := \overrightarrow{L}_p := (L_p^\sharp, L_p^\flat)$ the *p-adic L-vector of* E, and denote by $r_p^\natural$ the minimum of the orders of vanishing of $L_p^\sharp$ and $L_p^\flat$.

We would now like to find a pair of elements $\nu_\sharp$ and $\nu_\flat$ that give rise to regulators corresponding to our p-adic L-functions. Recall that $L_p^{PR}(E,T) = (L_p^\sharp, L_p^\flat)\mathcal{L}og_{\alpha,\beta}\begin{pmatrix} \nu_A \\ \nu_B \end{pmatrix}$.

Definition 5.20. — Let $M := \mathcal{L}og_{\alpha,\beta}(1+T)|_{T=0} = \mathcal{L}og_{\alpha,\beta}(1)$. We define

$$\begin{pmatrix} \nu_\sharp \\ \nu_\flat \end{pmatrix} := M \begin{pmatrix} \nu_A \\ \nu_B \end{pmatrix},$$

$$(N_\sharp, N_\flat) := (\nu_B, -\nu_A)\begin{pmatrix} (1-\frac{1}{\alpha})^2 & 0 \\ 0 & (1-\frac{1}{\beta})^2 \end{pmatrix} M^{-1} \times \det M.$$

Lemma 5.21. — *$\nu_\sharp, \nu_\flat, N_\sharp, N_\flat$ are in $D_p(E)$ and are not $\mathbb{Q}_p$-multiples of ω.*

Proof. — Calculation.

Definition 5.22. — We let $\mathrm{Reg}_\sharp := \mathrm{Reg}_{\frac{N_\sharp}{[\omega, N_\sharp]}}$ and $\mathrm{Reg}_\flat := \mathrm{Reg}_{\frac{N_\flat}{[\omega, N_\flat]}}$ be the regulators for the normalized heights associated to $N_\sharp$ and $N_\flat$. Also, we let

$$\mathrm{Reg}_p^\natural := \begin{cases} \Big((-a_p^2 + 2a_p + p - 1)\mathrm{Reg}_\sharp, \quad (-a_p + 2)\mathrm{Reg}_\flat \Big) & \text{for odd } p, \\ \Big((-a_p^3 + 2a_p^2 + 2pa_p - a_p - 2p)\mathrm{Reg}_\sharp, \quad (-a_p^2 + 2a_p + p - 1)\mathrm{Reg}_\flat \Big) & \text{for even } p. \end{cases}$$

We are now ready to give our p-adic version of BSD:

***Conjecture 5.23* (Tandem p-adic BSD).** — *Let E be an elliptic curve and p a prime of good reduction. Denote by $\overrightarrow{L}_p^*$ the first non-zero leading Taylor coefficient around $T = 0$ of the p-adic L-vector $\overrightarrow{L}_p = \overrightarrow{L}_p(E, T)$.*

1. *We have $r_p^\natural = r(E)$.*
2. $\overrightarrow{L}_p^* = \frac{\prod_v c_v \cdot \#\text{Ш}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tors})^2}\mathrm{Reg}_p^\natural(E/\mathbb{Q})$

Remark 5.24. — The term $\mathrm{Reg}_p^\natural(E/\mathbb{Q})$ is independent from the choice of Weierstraß equation. This follows from the proof of part 2 of Theorem 5.25, which only compares *coordinates* with respect to the basis ν_α, ν_β.

Theorem 5.25. — *This conjecture is equivalent to that of Mazur, Tate, Teitelbaum when p is ordinary, and that of Bernardi and Perrin-Riou when p is supersingular.*

Proof of equivalence for part 1. — Denote by r_p^α the order of vanishing of L_α. We now prove that $r_p^\alpha = r_p^\natural$ (which is enough even in the supersingular case, by Lemma 5.26).

We first prove that $r_p^\alpha \geqslant r_\natural$: For any non-negative integer $k < r_\natural$, denote the left column entries of $\mathcal{L}og_{\alpha,\beta}$ by $\log_\alpha^\sharp$ and $\log_\alpha^\flat$. Then by assumption and the product rule, we have

$$\frac{d^k}{dT^k}L_\alpha(T)\bigg|_{T=0} = \frac{d^k}{dT^k}\left(L_p^\sharp(T)\log_\alpha^\sharp(1+T) + L_p^\flat(T)\log_\alpha^\flat(1+T)\right)\bigg|_{T=0} = 0.$$

Now we prove that $r_p^\alpha \leqslant r_\natural$: When there is a non-negative integer $k < r_\natural$, we would like to prove that $\overrightarrow{L}_p^{(k)} = 0$, which we do by induction: For $k = 0$, note that $L_\alpha(0) = 0$ implies that its complex conjugate is zero: $\overline{L_\alpha(0)} = 0$. But we know that, as complex values, the right column of $\mathcal{L}og_{\alpha,\beta}(1)$ is the complex conjugate of the left column, so

$$(L_\alpha(0), \overline{L_\alpha(0)}) = \overrightarrow{L}_p(0)\mathcal{L}og_{\alpha,\beta}(1).$$

The claim follows from $\mathcal{L}og_{\alpha,\beta}(1)$ being invertible. Now suppose we know it up to $k-1$. Then we have

$$(L_\alpha^{(k)}(0), \overline{L_\alpha^{(k)}(0)}) = \overrightarrow{L}_p^{(k)}(0)\mathcal{L}og_{\alpha,\beta}(1) \tag{2}$$

again by the product rule and the fact that the right column of $\mathcal{L}og_{\alpha,\beta}(1)$ is the complex conjugate of the left column. So we may conclude that $\overrightarrow{L}_p^{(k)}(0) = 0$. *QED*

Proof for part 2. — From the equivalence of part 1 and the product rule, we have

$$\overrightarrow{L}_p^{*}\mathcal{L}og_{\alpha,\beta}(1) = \overrightarrow{L}_p^{*}M = (L_\alpha^*, \overline{L_\alpha^*}).$$

But we also have

$$(1-\varphi)^2(\mathrm{Reg}_{\frac{1}{\beta}}, \mathrm{Reg}_{\frac{1}{\alpha}})\begin{pmatrix} \nu_A \\ \nu_B \end{pmatrix} = \left(\frac{\widetilde{\mathrm{Reg}}_{\nu_B}}{[\omega,\nu_B]}, \frac{\widetilde{\mathrm{Reg}}_{\nu_A}}{[\omega,\nu_A]}\right)\begin{pmatrix} (1-\frac{1}{\alpha})^2 & 0 \\ 0 & (1-\frac{1}{\beta})^2 \end{pmatrix} M^{-1}\begin{pmatrix} \nu_\sharp \\ \nu_\flat \end{pmatrix}.$$

Since $[\omega,\nu_B] = [\nu_A,\nu_B] = -[\omega,\nu_A]$ and $\widetilde{\mathrm{Reg}}_\nu$ is linear in ν, this is equal to

$$\frac{1}{\det M}\left(\frac{1}{[\nu_A,\nu_B]}\widetilde{\mathrm{Reg}}_{N_\sharp}, \frac{-1}{[\nu_A,\nu_B]}\widetilde{\mathrm{Reg}}_{N_\flat}\right)\begin{pmatrix} \nu_\sharp \\ \nu_\flat \end{pmatrix} = \left(\frac{[\omega,N_\sharp]}{[\nu_\sharp,\nu_\flat]}\mathrm{Reg}_\sharp, \frac{-[\omega,N_\flat]}{[\nu_\sharp,\nu_\flat]}\mathrm{Reg}_\flat\right)\begin{pmatrix} \nu_\sharp \\ \nu_\flat \end{pmatrix}.$$

The rest follows from explicit calculation of the factors preceding the regulators. *QED*

Lemma 5.26. — *When p is supersingular,* $\mathrm{ord}_{T=0}L_p(E,\alpha,T) = \mathrm{ord}_{T=0}L_p(E,\beta,T)$.

Proof. — The same proof as in [**Po03**, Lemma 6.6] works.

Lemma 5.27. — *The value of the vector* $\left(L_p^\sharp(E,0), L_p^\flat(E,0)\right)$ *equals*

$$\begin{cases} (-a_p^2+2a_p+p-1, -a_p+2)\cdot\frac{L(E,1)}{\Omega_E} & \text{when } p \text{ is odd,} \\ (-a_p^3+2a_p^2+2pa_p-a_p-2p, -a_p^2+2a_p+p-1)\cdot\frac{L(E,1)}{\Omega_E} & \text{when } p \text{ is even.} \end{cases}$$

Proof. — This follows from the table after Corollary 3.13. *QED*

In particular this means that when $a_p = 2$ and p is odd, we may have $L_p^\flat(E,0) = 0$ while $L(E,1) \neq 0$. It thus seems reasonable to conjecture the following:

***Conjecture 5.28* (Separated p-adic BSD)**. — *Denote by $r_p^\sharp$ resp. $r_p^\flat$ the orders of vanishing of $L_p^\sharp$ resp. $L_p^\flat$, and by $L_p^{\sharp,*}$ resp. $L_p^{\flat,*}$ their non-zero leading terms at $T=0$.*

1.$\sharp$ **:** *When p is odd, $r_p^\sharp = r(E)$. When $p=2$,* $\begin{cases} r_p^\sharp = r(E) \text{ when } a_p \neq 1 \\ r_p^\sharp \geqslant r(E)+1 \text{ when } a_p = 1. \end{cases}$

1.$\flat$ **:** *When p is odd,* $\begin{cases} r_p^\flat = r(E) \text{ when } a_p \neq 2 \\ r_p^\flat \geqslant r(E)+1 \text{ when } a_p = 2. \end{cases}$ *When $p=2$, $r_p^\flat = r(E)$.*

2.$\sharp$ **:** *When p is odd or $a_p \neq 1$,* $L_p^{\sharp *} = \frac{\prod_v c_v\cdot\#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tors})^2}\widetilde{\mathrm{Reg}}_{\nu_\sharp}(E_\mathbb{Q})$.

2.$\flat$ **:** *When p is even or $a_p \neq 2$,* $L_p^{\flat *} = \frac{\prod_v c_v\cdot\#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tors})^2}\widetilde{\mathrm{Reg}}_{\nu_\flat}(E/\mathbb{Q})$.

Remark 5.29. — One can formulate these conjectures using the completed versions $\widehat{L}_p^\sharp$ and $\widehat{L}_p^\flat$, since we have $\mathcal{L}og_{\alpha,\beta}(1)\widehat{\mathcal{L}og}_{\alpha,\beta}(1)^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

To close this section, we state the following theorem of Kato:

***Theorem 5.30* ([Ka04], cf. [Ko03,** Theorem 9.4] **when** $a_p = 0$**)**

In Conjectures 5.23, 5.18, 5.16, 5.12, and even 5.28, the orders of vanishing of the p-adic L-functions are all $\geqslant r(E)$.

6. Consequences for modular forms and elliptic curves in the cyclotomic direction

In the last section, we have focused on the behavior at the point $T = 0$, but now scrutinize what happens when $T = \zeta_{p^n} - 1$ for $n \geqslant 1$. We estimate BSD-theoretic quantities in the cyclotomic direction, using the pairs of Iwasawa invariants of $L_p^\sharp$ and $L_p^\flat$ (which match those of $\widehat{L}_p^\sharp$ and $\widehat{L}_p^\flat$ when used, cf. Lemma 6.31).

Definition 6.1. — The (p-adic) analytic rank of $E(\mathbb{Q}_n)$ and of $E(\mathbb{Q}_\infty)$ are

$$r_n^{an} = \mathrm{rank}^{an} E(\mathbb{Q}_n) = \sum_{\zeta:\ p^n\text{th roots of unity}} \mathrm{ord}_{\zeta-1}(L_p(E,\alpha,T)),$$

$$r_\infty^{an} = \mathrm{rank}_\infty^{an} := \lim_{n\to\infty} \mathrm{rank}^{an} E(\mathbb{Q}_n) = \sum_{\zeta:\textit{all } p\text{-power roots of unity}} \mathrm{ord}_{\zeta-1}(L_p(E,\alpha,T)).$$

Note that by a theorem of Rohrlich [**Ro84**], this is a finite integer.

Definition 6.2. — We let d_n be the normalized jump in the ranks of E at level $\mathbb{Q}_n$:

$$d_n := \frac{\mathrm{rank} E(\mathbb{Q}_n) - \mathrm{rank} E(\mathbb{Q}_{n-1})}{p^n - p^{n-1}}$$

In what follows, denote by $D(\mathbb{Q}_n)$ the discriminant, by $R(E/\mathbb{Q}_n)$ the regulator, by $\mathrm{Tam}(E/\mathbb{Q}_n)$ the product of the Tamagawa numbers, and let $\Omega_{E/\mathbb{Q}_n} = (\Omega_{E/\mathbb{Q}})^{p^n}$.

***Conjecture 6.3* (Cyclotomic BSD)**. — *Let ζ_{p^n} be a primitive p^nth root of unity, d_n^{an} the order of vanishing of $L_p(E,\alpha,T)$ at $T = \zeta_{p^n} - 1$, and $r_n^{an'}$ the order of vanishing of the complex L-series $L(E/\mathbb{Q}_n, s)$. Then*

$$d_n^{an} = d_n \textit{ and } d_n^{an} = \frac{r_n^{an'} - r_{n-1}^{an'}}{p^n - p^{n-1}}.$$

In view of this conjecture, we put (cf. [**Ma71**, Remark 8.5]*):*

$$\#\text{Ш}^{an}(E/\mathbb{Q}_n) := \frac{L^{(r_n^{an'})}(E/\mathbb{Q}_n, 1)\#E^{tor}(\mathbb{Q}_n)^2\sqrt{D(\mathbb{Q}_n)}}{\Omega_{E/\mathbb{Q}_n} R(E/\mathbb{Q}_n)\mathrm{Tam}(E/\mathbb{Q}_n)}.$$

Our notation of d_n^{an}, which is independent of the choice ζ_{p^n}, is justified as follows:

Lemma 6.4. — *We have*

$$d_n^{an} = \frac{\mathrm{rank}^{an} E(\mathbb{Q}_n) - \mathrm{rank}^{an} E(\mathbb{Q}_{n-1})}{p^n - p^{n-1}}.$$

We postpone the proof until after Proposition 6.6.

Remark 6.5. — It is not clear how to relate the leading Taylor coefficient of $L_p(E,\alpha,T)$ at $T = \zeta_{p^n} - 1$ to the size of the Šafarevič-Tate groups in general (For a relative version, see [**MSD**, §9.5, Conjecture 4]).

6.1. The Mordell-Weil rank of an elliptic curve in the cyclotomic direction. — We now give an upper bound for the analytic rank of $E(\mathbb{Q}_n)$ in terms of $\lambda_\sharp$ and $\lambda_\flat$. When p is ordinary, we have the estimate $\lambda \geqslant \mathrm{rank}_\infty^{an}$, where λ is the λ-invariant of $L_p(E,\alpha,T)$. In appropriate cases (see Corollary 6.22), $\lambda = \lambda_\sharp$ or $\lambda = \lambda_\flat$. Consequently, this subsection is devoted to the more complicated scenario when p is supersingular.

Pollack proved the following proposition when $p \equiv 3 \mod 4$ and $a_p = 0$.

Proposition 6.6. — *Let $E/\mathbb{Q}$ be an elliptic curve and p be a prime of good supersingular reduction. If ζ is a p^nth root of unity, then we have*

$$\mathrm{ord}_{\zeta-1}L_p(E,\alpha,T) = \mathrm{ord}_{\zeta-1}L_p(E,\beta,T).$$

Proof. — Let $n=0$. Since $L_p^{(i)}(E,\alpha,T)$ and $L_p^{(i)}(E,\beta,T)$ are conjugate power series,

$$\mathrm{ord}_0 L_p(E,\alpha,T) = \mathrm{ord}_0 L_p(E,\beta,T).$$

Now let $n>0$. Let us first prove that $L_p(E,\alpha,\zeta-1)=0$ if and only if $L_p(E,\beta,\zeta-1)=0$: Recalling Definition 5.19, Observation 2.6 allows us to conclude that

$$\begin{aligned}&(L_p(E,\alpha,\zeta-1),L_p(E,\beta,\zeta-1)) = \overrightarrow{L}_p(E,\zeta-1)\mathcal{L}og_{\alpha,\beta}(\zeta-1)\\ &= \overrightarrow{L}_p(E,\zeta-1)\left(\begin{smallmatrix} * & * \\ * & * \end{smallmatrix}\right)\begin{pmatrix} 1 & 0 \\ 0 & \Phi_{p^n}(\zeta)\end{pmatrix}\begin{pmatrix} -1 & 11 \\ \alpha^{-1} & \beta^{-1}\end{pmatrix}\begin{pmatrix} \alpha^{-N} & 0 \\ 0 & \beta^{-N}\end{pmatrix}\\ &= \overrightarrow{L}_p(\zeta-1)\left(\begin{smallmatrix} * & * \\ * & * \end{smallmatrix}\right)\begin{pmatrix} 1 & 1 \\ \frac{-\Phi_{p^n}(\zeta)}{\alpha} & \frac{-\Phi_{p^n}(\zeta)}{\beta}\end{pmatrix}\begin{pmatrix} \alpha^{-n} & 0 \\ 0 & \beta^{-n}\end{pmatrix}\end{aligned}$$

for some 2×2-matrix $\left(\begin{smallmatrix} * & * \\ * & * \end{smallmatrix}\right)$ with entries in $\overline{\mathbb{Q}}$. But $\Phi_{p^n}(\zeta)=0$, so $L_p(E,\alpha,\zeta-1)=0$ implies that we have $\overrightarrow{L}_p(\zeta-1)\left(\begin{smallmatrix} * & * \\ * & * \end{smallmatrix}\right) = (0,*)$. Thus, we can conclude that $L_p(E,\beta,\zeta-1)=0$. A symmetric argument shows $L_p(E,\beta,\zeta-1)=0$ implies $L_p(E,\alpha,\zeta-1)=0$.

The rest is induction: Fixing $k \in$ and assuming $L_p^{(i)}(E,\alpha,\zeta-1) = L_p^{(i)}(E,\beta,\zeta-1) = 0$ for $0 \leqslant i < k$,

$$\left(L_p^{(k)}(E,\alpha,\zeta-1), L_p^{(k)}(E,\beta,\zeta-1)\right) = \overrightarrow{L}_p^{(k)}(E,\zeta-1)\mathcal{L}og_{\alpha,\beta}(\zeta-1)$$

by the product rule. By the above argument, we thus have

$$L_p^{(k)}(E,\alpha,\zeta-1)=0 \iff L_p^{(k)}(E,\beta,\zeta-1)=0.$$

QED

Corollary 6.7. — *Let $a_p=0$. Then we have* $\mathrm{rank}_\infty^{an} \leqslant \lambda_\sharp + \lambda_\flat$.

Definition 6.8. — Given an integer n, let Ξ_n be the matrix so that $\mathcal{L}og_{\alpha,\beta} = \mathcal{C}_1\cdots\mathcal{C}_n\Xi_n$.

Lemma 6.9. — *Fix and integer n and let $m \leqslant n$. We then have*

$$\mathrm{ord}_{\zeta_{p^m}-1}L_\alpha = j \textit{ if and only if } \mathrm{ord}_{\zeta_{p^m}-1}\overrightarrow{L}_p\mathcal{C}_1\cdots\mathcal{C}_n = j.$$

Proof. — Note that $\mathrm{ord}_{\zeta_{p^m}-1}L_\alpha = j$ if and only if $L(E,\alpha,\zeta_{p^m}-1)=0$ for $i \leqslant j-1$ but not $i=j$. But $\det \Xi_n(\zeta_{p^m}-1) \neq 0$, so it follows from induction on i and the product rule that this is equivalent to

$$\overrightarrow{L}_p^{(i)}\mathcal{C}_1\cdots\mathcal{C}_n(\zeta_{p^m}-1) = (0,0) \text{ for } i \leqslant j-1 \text{ but not } i=j,$$

which is equivalent to $\mathrm{ord}_{\zeta_{p^m}-1}\overrightarrow{L}_p\mathcal{C}_1\cdots\mathcal{C}_n = j$. *QED*

Proof of Lemma 6.4. — The entries of the vector $\overrightarrow{L}_p\mathcal{C}_1\cdots\mathcal{C}_n$ are up to units polynomials, so for $m \leqslant n$, we have $\mathrm{ord}_{\zeta_{p^m}-1}\overrightarrow{L}_p\mathcal{C}_1\cdots\mathcal{C}_n = \mathrm{ord}_{\zeta'_{p^m}-1}\overrightarrow{L}_p\mathcal{C}_1\cdots\mathcal{C}_n$ for any two primitive p^mth roots of unity ζ_{p^m} and ζ'_{p^m}. From Lemma 6.9, $\mathrm{ord}_{\zeta_{p^m}-1}L_\alpha = \mathrm{ord}_{\zeta'_{p^m}-1}L_\alpha$. *QED*

Proof. — The proof of [**Po03**, Corollary 6.8] works because of Proposition 6.6. *QED*

Notation 6.10. — Given $x \in \mathbb{Q}$, we let $\lfloor x \rfloor$ be the largest integer $\leqslant x$.

Definition 6.11. — The nth **$\sharp/\flat$-Kurihara term** $q_n^{\sharp/\flat}$ is given by:

$$q_n^\sharp := \left\lfloor \frac{p^n}{p+1} \right\rfloor = p^{n-1} - p^{n-2} + p^{n-3} - p^{n-4} + \cdots + p^2 - p \text{ if } n \text{ is odd.}$$

$$q_n^\flat := \left\lfloor \frac{p^n}{p+1} \right\rfloor = p^{n-1} - p^{n-2} + p^{n-3} - p^{n-4} + \cdots + p - 1 \text{ if } n \text{ is even.}$$

We also define $q_n^\sharp := q_{n+1}^\sharp$ for even n, and $q_n^\flat := q_{n+1}^\flat$ for odd n. Finally, put

$$\nu_\sharp := \text{largest odd integer } n \geqslant 1 \text{ so that } \lambda_\sharp \geqslant p^n - p^{n-1} - q_n^\sharp,$$

$$\nu_\flat := \text{largest even integer } n \geqslant 2 \text{ so that } \lambda_\flat \geqslant p^n - p^{n-1} - q_n^\flat.$$

In case no such integer exists, we put $\nu_\sharp := 0$ resp. $\nu_\flat := 0$.

Proposition 6.12. — *Let* $\nu = \max(\nu_\sharp, \nu_\flat)$. *We have* $\mathrm{rank}_\infty^{an} \leqslant \min(q_\nu^\sharp + \lambda_\sharp, q_\nu^\flat + \lambda_\flat)$.

Proof. — In the proof, we justify the two equality signs in the following equation:

$$\sum_{\substack{\text{all } p\text{-power} \\ \text{roots of unity } \zeta}} \mathrm{ord}_{\zeta-1}L_\alpha = \sum_{\substack{\zeta \text{ so that } \zeta^{p^n}=1 \\ \text{and } n\leqslant\max(\nu_\sharp,\nu_\flat)}} \mathrm{ord}_{\zeta-1}L_\alpha = \sum_{\substack{\zeta \text{ so that } \zeta^{p^n}=1 \\ \text{and } n\leqslant\max(\nu_\sharp,\nu_\flat)}} \mathrm{ord}_{\zeta-1}\overrightarrow{L}_p\mathcal{C}_1\cdots\mathcal{C}_{\max(\nu_\sharp,\nu_\flat)}$$

The result then follows on noting that the last term is bounded by the maximum of the λ-invariants of the components of $\overrightarrow{L}_p\mathcal{C}_1\cdots\mathcal{C}_{\max(\nu_\sharp,\nu_\flat)}$, which are

$$\begin{cases} \lambda_\sharp + q_n^\sharp \text{ and } \lambda_\flat + q_n^\flat \text{ if } n \text{ is even,} \\ \lambda_\flat + q_n^\flat \text{ and } \lambda_\sharp + q_n^\sharp \text{ if } n \text{ is odd.} \end{cases}$$

We justify the first equality sign. By Proposition 6.6, $\mathrm{ord}_{\zeta_{p^n}-1}L_\alpha = \mathrm{ord}_{\zeta_{p^n}-1}L_\beta$. Since $\det \Xi_n|_{T=\zeta_{p^n}-1} \neq 0$, $\mathrm{ord}_{\zeta_{p^n}-1}L_\alpha > 0$ if and only if $\overrightarrow{L}_p\mathcal{C}_1\cdots\mathcal{C}_n\Big|_{T=\zeta_{p^n}-1} = (0,0)$. Thus, $\mathrm{ord}_{\zeta_{p^n}-1}L_\alpha > 0$ implies

$$\begin{cases} \lambda_\flat + q_n^\flat \geqslant p^n - p^{n-1} \text{ if } n \text{ is even,} \\ \lambda_\sharp + q_n^\sharp \geqslant p^n - p^{n-1} \text{ if } n \text{ is odd.} \end{cases}$$

Conversely, $\lambda_\flat < p^n - p^{n-1} - q_n^\flat$ for some even n implies $\lambda_\flat < p^m - p^{m-1} - q_m^\flat$ for any even $m \geqslant n$, which implies $\mathrm{ord}_{\zeta_{p^m}-1} L_\alpha = 0$.

Similarly, $\lambda_\sharp < p^n - p^{n-1} - q_n^\sharp$ for some odd n implies $\mathrm{ord}_{\zeta_{p^m}-1} L_\alpha = 0$ for any odd $m \geqslant n$, so

$$m > \max(\nu_\sharp, \nu_\flat) \text{ implies } \mathrm{ord}_{\zeta_{p^m}-1} L_\alpha = 0.$$

The second equality sign follows from Lemma 6.9 applied to $n = \max(\nu_\sharp, \nu_\flat)$. *QED*

We thank Robert Pollack for pointing out an example in which the sum of the lambda-invariants is not a bound for $\mathrm{rank}_\infty^{an}$ as in Corollary 6.1. Our proposition explains the bound:

Example 6.13. — *Consider E37A. For the prime* 3*, we have* $a_3 = -3$*, and at this prime* 3*, we have* $\lambda_\sharp = 1$*, while* $\lambda_\flat = 5$*, and* $\mathrm{rank}_\infty = 7$*. In this case* $\nu_\sharp = 0$ *and* $\nu_\flat = 2$*. Thus, the bound for* $\mathrm{rank}_\infty^{an}$ *is* $\min(q_2^\flat + 5, q_2^\sharp + 1) = \min(3 - 1 + 5, 3^2 - 3 + 1) = 7$*. Note that* $\mathrm{rank}_\infty^{an} = 7 > \lambda_\sharp + \lambda_\flat = 6$.

6.2. The greatest common divisor.

— *We now generalize and give some evidence for the following conjecture found in* [**KP07**, Problem 3.2].

***Conjecture 6.14* (The problem of Kurihara and Pollack).** — *Let* $E/\mathbb{Q}$ *be an elliptic curve so* p *is a prime of good reduction and* $a_p = 0$*. Then*

$$\gcd(L_p^\sharp(E,T), L_p^\flat(E,T)) = \left(T^{r_0} \prod_{d_n \geqslant 1 \text{ and } n \geqslant 1} \Phi_{p^n}^{d_n - 1}(1+T) \right).$$

Note that this is an equality of *ideals*, since the greatest common divisor of two functions of $\mathbb{Q} \otimes {}_p[[T]]$ is only well-defined as a ${}_p[[T]]$-ideal. We can give the following proposition:

Proposition 6.15. — *Let* $E/\mathbb{Q}$ *be an elliptic curve and* p *a prime of good reduction. For some polynomial* $P_{\text{Ш}}(E,T)$ *that doesn't vanish at* $T = \zeta_{p^n} - 1$ *for any* $n \geqslant 0$,

$$\gcd\left(L_p^\sharp(E,T), L_p^\flat(E,T)\right) = \left(P_{\text{Ш}}(E,T) \cdot T^{r_0^{an}} \prod_{d_n \geqslant 1 \text{ and } n \geqslant 1} \Phi_{p^n}^{\epsilon_n^{an} - 1}(1+T) \right),$$

where $\epsilon_n^{an} - 1 = d_n^{an} - 1$ *or* $\epsilon_n^{an} - 1 = d_n^{an}$*, and* $P_{\text{Ш}}(E,T)$ *has no zeroes at* $T = \zeta_{p^n - 1}$ *for* $n \geqslant 0$.

Convention 6.16. — Given a vector $(f(T), g(T))$ of p-adic analytic functions, we define its order of vanishing at s by $\mathrm{ord}_{T=s}(f(T), g(T)) := \min(\mathrm{ord}_{T=s} f(T), \mathrm{ord}_{T=s} g(T))$.

Lemma 6.17. — *Denote by* ι *complex conjugation. Let* $f(T), g_1(T)$*,* $g_2(T)$*, and the entries of a* 2×2 *matrix* $M(T)$ *be* p*-adic analytic functions on the open unit disk and* $e = \mathrm{ord}_{T=s} f(s)$ *so that*

$$(f(T), \iota(f(T))) = (g_1(T), g_2(T)) M(T)$$

and $\det M(s) \neq 0$*. Then we have* $\mathrm{ord}_{T=s}(g_1(T), g_2(T)) = e$.

Proof. — By calculus, $\left(f^{(m)}(s), \iota\left(f^{(m)}(s)\right)\right) = (0,0)$ if and only if $(g_1^{(m)}(s), g_2^{(m)}(s)) = (0,0)$ for $m \geqslant 0$. *QED*

Corollary 6.18. — *The exact power of T dividing* $\gcd\left(L_p^\sharp(E,T), L_p^\flat(E,T)\right)$ *is* $T^{r_0^{an}}$.

Lemma 6.19. — *Let $f_1(T), f_2(T), g_1(T), g_2(T)$ be analytic functions on the open unit disk and put*

$$\overrightarrow{f}(T) = (f_1(T), f_2(T)) \textit{ and } \overrightarrow{g}(T) = (g_1(T), g_2(T))$$

so that

$$\overrightarrow{f}(T) = \overrightarrow{g}(T)\begin{pmatrix} a_p & p \\ -\Phi_{p^n}(1+T) & 0 \end{pmatrix}.$$

Then $\mathrm{ord}_{T=s}\overrightarrow{g}(T) = \mathrm{ord}_{T=s}\overrightarrow{f}(T)$ *or* $\mathrm{ord}_{T=s}\overrightarrow{g}(T) = \mathrm{ord}_{T=s}\overrightarrow{f}(T) - 1$.

Proof. — Since $\mathrm{ord}_{T=s}g_1(T) = \mathrm{ord}_{T=s}f_2(T)$ and $a_p g_1(T) - f_1(T) = -\Phi_{p^n}(1+T)g_2(T)$,

$$\text{if } \begin{cases} \mathrm{ord}_{T=s}f_1(T) < \mathrm{ord}_{T=s}f_2(T), \text{ then } \mathrm{ord}_{T=s}g_2(T) = \mathrm{ord}_{T=s}f_1(T) - 1 \\ \mathrm{ord}_{T=s}f_1(T) = \mathrm{ord}_{T=s}f_2(T) \text{ and } a_p \neq 0, \text{ then } \mathrm{ord}_{T=s}g_2(T) \geqslant \mathrm{ord}_{T=s}f_1(T) - 1 \\ \mathrm{ord}_{T=s}f_1(T) > \mathrm{ord}_{T=s}f_2(T) \text{ and } a_p \neq 0, \text{ then } \mathrm{ord}_{T=s}g_2(T) = \mathrm{ord}_{T=s}f_2(T) - 1 \\ \mathrm{ord}_{T=s}f_1(T) \geqslant \mathrm{ord}_{T=s}f_2(T) \text{ and } a_p = 0, \text{ then } \mathrm{ord}_{T=s}g_2(T) = \mathrm{ord}_{T=s}f_1(T) - 1 \end{cases}$$

QED

Proof of Theorem 6.15. — We use Corollary 6.18 and the following argument: Let $M = I$ when $n = 1$ and $M = \mathcal{C}_1 \cdots \mathcal{C}_{n-1}$ when $n > 1$. Recall that $\overrightarrow{L}_p = \left(L_p^\sharp, L_p^\flat\right)$, so that

$$(L_p(E,\alpha,T), L_p(E,\beta,T)) = \overrightarrow{L}_p M \mathcal{C}_n \Xi_n.$$

From Lemma 6.17, $\mathrm{ord}_{T=\zeta_{p^n}-1}\left(\overrightarrow{L}_p M\mathcal{C}_n\right) = d_n^{an}$. Lemma 6.19 then implies $\mathrm{ord}_{T=\zeta_{p^n}-1}\left(\overrightarrow{L}_p M\right) = d_n^{an} - 1$ or $\mathrm{ord}_{T=\zeta_{p^n}-1}\left(\overrightarrow{L}_p M\right) = d_n^{an}$. From $\det M(\zeta_{p^n}-1) \neq 0$ and the product rule, $\mathrm{ord}_{T=\zeta_{p^n}-1}\overrightarrow{L}_p = d_n^{an} - 1$ or $\mathrm{ord}_{T=\zeta_{p^n}-1}\overrightarrow{L}_p = d_n^{an}$. *QED*

We therefore make the following conjecture:

Conjecture 6.20. — *Let $E/\mathbb{Q}$ be an elliptic curve, and p a good prime. Then*

$$\gcd(L_p^\sharp(E,T), L_p^\flat(E,T)) = \left(T^{r_0} \prod_{d_n \geqslant 1 \textit{ and } n \geqslant 1} \Phi_{p^n}^{d_n - 1}(1+T)\right).$$

6.3. The special value of the L-function of f in the cyclotomic direction. — In this section, we prove a special value formula for modular forms of weight two. Formulating the precise statement is a little subtle, so we first give an explicit version of the main theorem in the case of elliptic curves (where the special value is dressed as the analytic size of the Šafarevič-Tate group). After that, we state it for general modular forms of weight two, before finally giving the proof.

6.3.1. Growth of the Šafarevič-Tate group in the cyclotomic direction. — In the case of an elliptic curve, we estimate the p-part of the analytic size of the Šafarevič-Tate group:

$$\#Ш^{an}(E/\mathbb{Q}_n) := \frac{L^{(r_n^{an'})}(E/\mathbb{Q}_n,1)\#E^{tor}(\mathbb{Q}_n)^2\sqrt{D(\mathbb{Q}_n)}}{\Omega_{E/\mathbb{Q}_n}R(E/\mathbb{Q}_n)\mathrm{Tam}(E/\mathbb{Q}_n)}$$

Recall that r_∞^{an} denotes the p-adic analytic rank of $E(\mathbb{Q}_\infty)$.

Theorem 6.21. — *Let E be an elliptic curve and p be a prime of good reduction. We denote by $\mu_{\sharp/\flat}$ and $\lambda_{\sharp/\flat}$ the Iwasawa invariants of $L_p^\sharp(E,T)$ and $L^\flat(E,T)$, and put also $e_n := \mathrm{ord}_p(\#Ш^{an}(E/\mathbb{Q}_n))$. Then for $n \gg 0$, we have the following formulas for $e_n - e_{n-1}$:*

- *If $\mu_\sharp = \mu_\flat$ and $p|a_p$, or if $a_p = 0$, we have*
$$e_n - e_{n-1} = \begin{cases} (p^n - p^{n-1})\mu_\sharp + \lambda_\sharp - r_\infty^{an} + q_n^\sharp \text{ if } n \text{ is odd,} \\ (p^n - p^{n-1})\mu_\flat + \lambda_\flat - r_\infty^{an} + q_n^\flat \text{ if } n \text{ is even.} \end{cases}$$
- *If $\mu_\sharp - \mu_\flat \leqslant -1$ and $\mathrm{ord}_p(a_p) = 1$, then*
$$e_n - e_{n-1} = (p^n - p^{n-1})\mu_\sharp + \lambda_\sharp - r_\infty^{an} + q_n^\sharp.$$
- *If $\mu_\sharp - \mu_\flat \geqslant 1$ and $\mathrm{ord}_p(a_p) = 1$, then*
$$e_n - e_{n-1} = (p^n - p^{n-1})\mu_\flat + \lambda_\flat - r_\infty^{an} + q_n^\flat.$$
- *Let $p \nmid a_p$. If $\mu_\sharp < \mu_\flat$, or $\mu_\sharp = \mu_\flat$ and $\lambda_\sharp - \lambda_\flat < p-1$, we have*
$$e_n - e_{n-1} = (p^n - p^{n-1})\mu_\sharp + \lambda_\sharp - r_\infty^{an}.$$
- *Let $p \nmid a_p$. If $\mu_\sharp > \mu_\flat$, or $\mu_\sharp = \mu_\flat$ and $\lambda_\sharp - \lambda_\flat > p-1$, we have*
$$e_n - e_{n-1} = (p^n - p^{n-1})\mu_\flat + \lambda_\flat - r_\infty^{an}.$$

Moreover, if $\mathrm{ord}_p(L(E,1)/\Omega_E) = 0$, $a_p \not\equiv 1 \mod p$, p is odd, and $p \nmid \mathrm{Tam}(E/\mathbb{Q}_n)$, then $e_0 = e_1 = 0 = \mu_{\sharp/\flat} = \lambda_{\sharp/\flat} = e_\infty^{an}$ and the above formulas are valid for $n \geqslant 2$.

Proof. — This follows from Theorem 6.29 in the same way that [**Po03**, Proposition 6.10] follows from [**Po03**, Proposition 6.9 (3)]: The idea is to pick n large enough so that $\mathrm{ord}_p(\#E(\mathbb{Q}_n)) = \mathrm{ord}_p(\#E(\mathbb{Q}_{n-1}))$, $L(E,\chi,1) \neq 0$ for χ of order p^n, and $\mathrm{ord}_p(\mathrm{Tam}(E/\mathbb{Q}_n)) = \mathrm{ord}_p(\mathrm{Tam}(E/\mathbb{Q}_{n-1}))$. For the purposes of the last claim, we can pick $n = 0$ by [**Ku02**, Proposition 1.2] and the arguments of its proof, invoking [**Gr99**, Proposition 3.8] and Theorem 3.11. Noting that $R(E/\mathbb{Q}_n) = p^{r_n}R(E/\mathbb{Q}_{n-1})$ and by computing $D(\mathbb{Q}_n)$,

$$\begin{aligned} e_n - e_{n-1} &= \mathrm{ord}_p\left(\prod\nolimits_{\chi \text{ of order } p^n} \tfrac{L(E/\mathbb{Q},\chi^{-1},1)}{\Omega_{E/\mathbb{Q}}}\right) + p^{n-1}(p-1)\cdot\tfrac{n+1}{2} - r_\infty^{an} \\ &= \mathrm{ord}_p\left(\prod\nolimits_{\chi \text{ of order } p^n} \tau(\chi)\tfrac{L(E/\mathbb{Q},\chi^{-1},1)}{\Omega_{E/\mathbb{Q}}}\right) - r_\infty^{an}. \end{aligned}$$

QED

In the supersingular case, Theorem 6.21 generalizes [**Po03**, Proposition 6.10], which works under the assumption $a_p = 0$. For an algebraic version of this Theorem 6.21 for supersingular primes, see [**Ko03**, Theorem 10.9] in the case $a_p = 0$ and odd p, and [**Sp13**, Theorem 3.13] for any odd supersingular prime.

In the ordinary case, the estimate for $n \gg 0$ is

$$e_n - e_{n-1} = (p^n - p^{n-1})\mu + \lambda - r_\infty^{an},$$

where μ and λ are the Iwasawa invariants of $L_p(E, \alpha, T)$. Thus, we obtain

Corollary 6.22. — *In the ordinary case, let λ be the λ-invariant of $L_p(E, \alpha, T)$. Then*

$$\lambda = \begin{cases} \lambda_\sharp \text{ when } \mu_\sharp < \mu_\flat \text{ or } \mu_\sharp = \mu_\flat \text{ and } \lambda_\sharp < \lambda_\flat + p - 1 \\ \lambda_\flat \text{ when } \mu_\flat < \mu_\sharp \text{ or } \mu_\flat = \mu_\sharp \text{ and } \lambda_\flat < \lambda_\sharp + 1 - p. \end{cases}$$

Conjecture 6.23. — *In the above setting, we have*

$$\lambda = \lambda_\sharp = \lambda_\flat \text{ if } \mu_\sharp = \mu_\flat \text{ and } \lambda_\sharp = \lambda_\flat + p - 1.$$

Remark 6.24. — These formulas are compatible with Perrin-Riou's formulas in [**PR03**]. Note that she assumes that p is odd, and that $\mu_+ = \mu_-$ or $a_p = 0$ in [**PR03**, Theorem 6.1(4)], cf. also [**Sp13**, Theorem 5.1] . Her invariants match ours by Corollary 6.31. For $p = 2$, our results are compatibile with [**KO06**, Theorem 0.1 (2)] (which determines the structure of the 2-primary component of Ш$(E/\mathbb{Q}_n)$ under the assumption $a_2 = \pm 2$ and other conditions, which force the Iwasawa invariants to vanish).

6.3.2. The special values for modular forms. —

Definition 6.25. — Put

$$\mathcal{C}_i(a, 1+T) := \begin{pmatrix} a & 1 \\ -\epsilon(p)\Phi_{p^i}(1+T) & 0 \end{pmatrix}.$$

We now put $\mathcal{H}_a^i(1+T) := \mathcal{C}_1(a, 1+T) \cdots \mathcal{C}_i(a, 1+T)$.

Definition 6.26. — Given an element a in the closed unit disk of ${}_p$, let $v := \mathrm{ord}_p(a) \geqslant 0$. When $v > 0$, let $k \in {}^{\geqslant 1}$ be the smallest positive integer so that $v \geqslant \frac{p^{-k}}{2}$. We now let v_m be the upper left entry in the valuation matrix of $\mathcal{H}_a^m(\zeta_{p^{k+2}} - 1)$.

Given further an integer n, we now define two functions $f_{*,n}(v, v_2)$ for $* \in \{\sharp, \flat\}$ so that they are *continuous* in $v \in [0, \infty]$ and in $v_2 \in [2v, \infty]$.

When $\infty > v > 0$, we put $\delta := \min(v_2 - 2v, (p-1)p^{-k-2})$. Note that $\delta = 0$ when $2v \neq \frac{p^{-k}}{2}$. We define

$$f_{\sharp,n}(v, v_2) := \begin{cases} (p^n - p^{n-1})kv + \left\lfloor \frac{p^{n-k}}{p+1} \right\rfloor & \text{when } n \not\equiv k \mod (2) \\ (p^n - p^{n-1})\left((k-1)v + \delta\right) + \left\lfloor \frac{p^{n+1-k}}{p+1} \right\rfloor & \text{when } n \equiv k \mod (2), \end{cases}$$

$$f_{\flat,n}(v, v_2) := \begin{cases} (p^n - p^{n-1})\left((k-1)v + \delta\right) + p\left\lfloor \frac{p^{n-k}}{p+1} \right\rfloor + p - 1 & \text{when } n \not\equiv k \mod (2) \\ (p^n - p^{n-1})kv + p\left\lfloor \frac{p^{n-1-k}}{p+1} \right\rfloor + p - 1 & \text{when } n \equiv k \mod (2). \end{cases}$$

Note that the tail terms $\left\lfloor \frac{p^{n-k}}{p+1} \right\rfloor$ (resp. $\left\lfloor \frac{p^{n+1-k}}{p+1} \right\rfloor$) appearing in $f_{\sharp,n}(v,v_2)$ are equal to $q^\sharp_{n-k}$. For $n>k$, those for $f_{\flat,n}(v,v_2)$, i.e. $p\left\lfloor \frac{p^{n-k}}{p+1} \right\rfloor + p-1$ and $p\left\lfloor \frac{p^{n-1-k}}{p+1} \right\rfloor + p-1$, are both $q^\flat_{n-k}$. For $v=\infty$, we define

$$f_{*,n}(\infty,v_2) := \lim_{v\to\infty} f_{*,n}(v,v_2).$$

Finally, for $v=0$, we similarly put

$$f_{*,n}(0,v_2) := \lim_{v\to 0} f_{*,n}(v,v_2) = \begin{cases} 0 & \text{when } *=\sharp \\ p-1 & \text{when } *=\flat. \end{cases}$$

(We use this seemingly strange adherence to the symbol v_2 simply for uniform notation.)

Definition 6.27. — The **sporadic case** occurs if $v=0$ and $\mu_\sharp=\mu_\flat$ and $\lambda_\sharp=\lambda_\flat+p-1$, or if $v=\frac{p^{-k}}{2}$ and $v_2=2v(1+p^{-1}-p^{-2})$ and

$$\begin{cases} n\not\equiv k \mod 2 \text{ and } \begin{cases} \mu_\sharp-\mu_\flat > v-\frac{2v}{p^3+p^2} \text{ or} \\ \mu_\sharp-\mu_\flat = v-\frac{2v}{p^3+p^2} \text{ and } \lambda_\sharp>\lambda_\flat, \text{ or} \end{cases} \\ n\equiv k \mod 2 \text{ and } \begin{cases} \mu_\sharp-\mu_\flat < \frac{2v}{p^3+p^2}-v \text{ or} \\ \mu_\sharp-\mu_\flat = \frac{2v}{p^3+p^2}-v \text{ and } \lambda_\sharp\leqslant\lambda_\flat. \end{cases} \end{cases}$$

Definition 6.28 **(Modesty Algorithm).** — Given a in the closed unit disk, an integer n, integers $\lambda_\sharp$ and $\lambda_\flat$, and rational numbers $\mu_\sharp$ and $\mu_\flat$, choose $*\in\{\sharp,\flat\}$ via

$$*=\begin{cases} \sharp \text{ if } (p^n-p^{n-1})\mu_\sharp+\lambda_\sharp+f_{\sharp,n}(v,v_2) < (p^n-p^{n-1})\mu_\flat+\lambda_\flat+f_{\flat,n}(v,v_2) \\ \flat \text{ if } (p^n-p^{n-1})\mu_\flat+\lambda_\flat+f_{\flat,n}(v,v_2) < (p^n-p^{n-1})\mu_\sharp+\lambda_\sharp+f_{\sharp,n}(v,v_2). \end{cases}$$

Theorem 6.29. — *Let f be a modular form of weight two which is a normalized eigenform for all T_n, and p a prime of good reduction. Define the terms of Definition 6.26 by letting $a:=a_p$, the eigenvalue of T_p. Let χ be a character of $\;^\times_p$ with order p^n. Denote by $\tau(\chi)$ the Gauß sum. Let n be large enough so that $\operatorname{ord}_p(L_p^{\sharp/\flat}(f,\zeta_{p^n}-1))=\mu^{\sharp/\flat}+\frac{\lambda^{\sharp/\flat}}{p^n-p^{n-1}}$ and $n>k$, and suppose we are not in the sporadic case. Then*

$$\operatorname{ord}_p(\tau(\chi)\frac{L(f,\chi^{-1},1)}{\Omega_f}) = \frac{g_n}{p^n-p^{n-1}}, \text{ where } g_n=(p^n-p^{n-1})\mu_*+\lambda_*+f_{*,n}(v,v_2),$$

and $*\in\{\sharp,\flat\}$ is chosen according to the modesty algorithm.

Proof. — Let p be odd, since the other case is similar. Letting $\chi(\gamma)=\zeta_{p^n}$, the interpolation property implies

$$L_p^{an}(f,\alpha,\zeta_{p^n}-1) = \frac{1}{\alpha^{n+1}}\frac{p^{n+1}}{\tau(\chi^{-1})}\frac{L(f,\chi^{-1},1)}{\Omega_f}.$$

Now $\alpha^{n+1}L_p(f,\alpha,\zeta_{p^n}-1)$ has the desired p-adic valuation by Proposition 6.32 and Theorem 1.13. *QED*

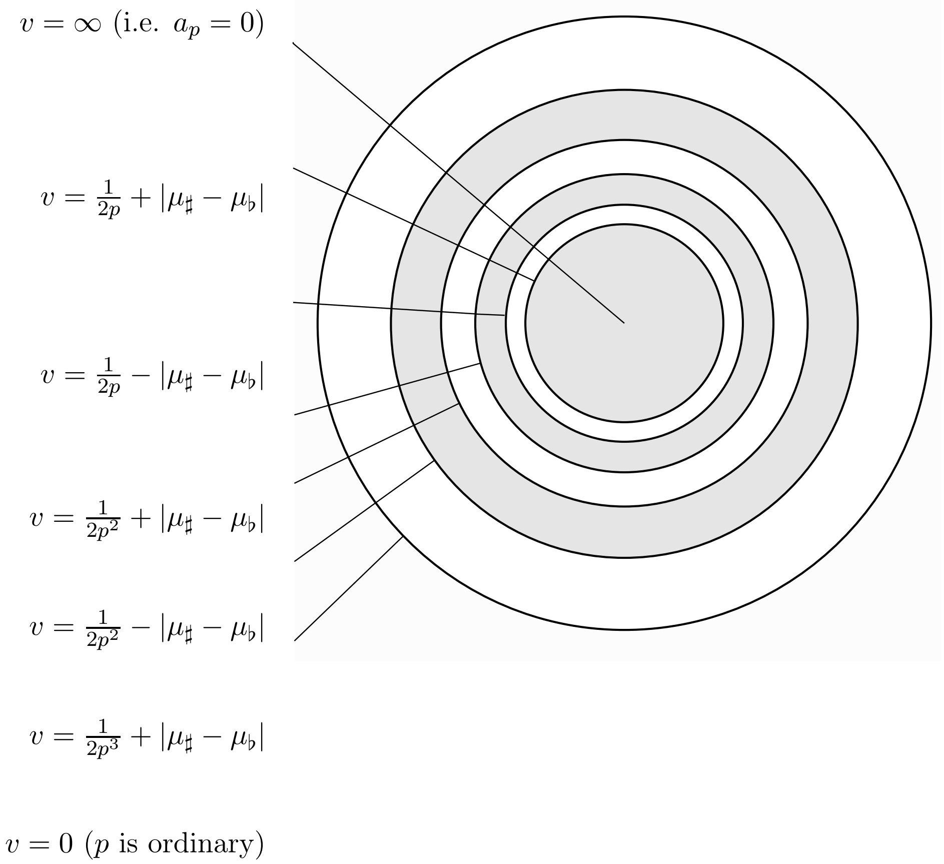
$v = \infty$ (i.e. $a_p = 0$)
$v = \frac{1}{2p} + |\mu_\sharp - \mu_\flat|$
$v = \frac{1}{2p} - |\mu_\sharp - \mu_\flat|$
$v = \frac{1}{2p^2} + |\mu_\sharp - \mu_\flat|$
$v = \frac{1}{2p^2} - |\mu_\sharp - \mu_\flat|$
$v = \frac{1}{2p^3} + |\mu_\sharp - \mu_\flat|$
$v = 0$ (p is ordinary)

FIGURE 1. The locus inside the p-adic unit disk in which the modesty algorithm chooses $\sharp$ or $\flat$ when $\frac{p-1}{4p^4} < |\mu_\sharp - \mu_\flat| < \frac{p-1}{4p^3}$.

Here, $v = \mathrm{ord}_p(a_p)$ indicates the possible valuations of a_p inside the unit disk. At the center, we have $a_p = 0$, i.e. $v = \infty$. On the edge, we have $v = 0$, so that p is ordinary.

In the central shaded region, the formula involves $\mu_\sharp$, $\lambda_\sharp$ for odd n and $\mu_\flat$, $\lambda_\flat$ for even n, while in the second shaded region, $\mu_\sharp$ and $\lambda_\sharp$ are part of the formula for even n, and $\mu_\flat$ and $\lambda_\flat$ for odd n. In the outermost shaded region, the roles are flipped yet again and the $\sharp$-invariants come into play for odd n, and the $\flat$-invariants for even n.

When $\mu_\sharp < \mu_\flat$, the formulas are only controlled by the $\mu_\sharp$ and $\lambda_\sharp$ in the non-shaded regions.

***Definition 6.30* (The invariants $\mu_\pm$ and $\lambda_\pm$ due to Perrin-Riou, resp. Greenberg, Iovita, and Pollack)**

Let p be a supersingular prime, and let p be odd [(5)]. Let $(Q_n)_n \in \Lambda_n$ be a queue sequence. Let π be a generator of the maximal ideal of so that $\pi^m = p$. When $Q_n \neq 0$, we define $\mu'(Q_n)$ to be the unique integer so that

$$Q_n \in (\pi)^{\mu'(Q_n)}\Lambda_n - (\pi)^{\mu'(Q_n)+1}\Lambda_n.$$

[(5)] This is an assumption that Perrin-Riou makes. For $p = 2$, one could define the $\mu_\pm$ and $\lambda_\pm$ in the same way but switch the signs so that they agree with the Iwasawa invariants of $L_p^\pm$ in the case $a_p = 0$.

Further, we let $\lambda(Q_n)$ be the unique integer so that $\pi^{-\mu'(Q_n)}Q_n \mod \pi \in \tilde{I_n}^{\lambda(Q_n)} - \tilde{I_n}^{\lambda(Q_n)+1}$, where $\tilde{I_n}$ is the augmentation ideal of $/\pi[\Gamma_n]$. Finally, we put $\mu(Q_n) := m\mu'(Q_n)$. Then for even (resp. odd) n, $\mu(Q_n)$ stabilizes to a minimum constant value μ_+ (resp. μ_-). When $\mu_+ = \mu_-$, put

$$\lambda_+ := \lim_{n\to\infty} \lambda(Q_{2n}) - q^\flat_{2n} \text{ and } \lambda_- := \lim_{n\to\infty} \lambda(Q_{2n+1}) - q^\sharp_{2n+1}.$$

Corollary 6.31. — *Suppose $\mu_\sharp$ and $\lambda_\sharp$ (resp. $\mu_\flat$ and $\lambda_\flat$) appear in the estimates of Theorem 6.29. Then they are the Iwasawa invariants of $\widehat{L}_p^\sharp$ (resp. of $\widehat{L}_p^\flat$). When $\mu_\sharp = \mu_\flat$, we define $\mu_\pm$ and $\lambda_\pm$ via the queue sequences that gave rise to $L_p^\sharp$ and $L_p^\flat$, and have*

$$\mu_\sharp = \mu_+, \lambda_\sharp = \lambda_+, \mu_\flat = \mu_-, \text{ and } \lambda_\flat = \lambda_-.$$

Proof. — The Kurihara terms $f_{*,n}(v, v_2)$ come from appropriate valuation matrices of $\mathcal{L}og_{\alpha,\beta}$ and $\widehat{\mathcal{L}og}_{\alpha,\beta}$, which are the same. Thus, the Iwasawa invariants of $\widehat{L}_p^{\sharp/\flat}$ and of $L_p^{\sharp/\flat}$ match. We can calculate the p-part of the special value in Theorem 6.29 using the appropriate queue sequences [(6)]. Since $\mu_+ = \mu_-$, we are a posteriori not in the sporadic case, so that our formulas match. *QED*

6.3.3. Tools for the proof of Theorem 6.29. —

Proposition 6.32. — *Suppose we have $(L^\sharp(T), L^\flat(T)) \in [[T]]^{\oplus 2}$, where is the ring of integers of some finite extension of $\mathbb{Q}_p$. Rewrite $L^\sharp(T) := p^{\mu_\sharp} \times P^\sharp(T) \times U^\sharp(T)$ for a distinguished polynomial $P^\sharp(T)$ with λ-invariant $\lambda_\sharp$ and a unit $U^\sharp(T)$. Note that $\mu_\sharp \in \mathbb{Q}$. Rewrite $L^\flat(T)$ similarly to extract $\mu_\flat$ and $\lambda_\flat$. Suppose we are not in the sporadic case. Let a and k be as in Definition 6.26, and e_n the left entry of the 1×2 valuation matrix of*

$$(L^\sharp(\zeta_{p^n} - 1), L^\flat(\zeta_{p^n} - 1))\mathcal{H}_a^{n-1}(\zeta_{p^n} - 1).$$

Then for n large enough so that $n > k$ and $\text{ord}_p(L^{\sharp/\flat}(\zeta_{p^n} - 1)) = \mu^{\sharp/\flat} + \frac{\lambda^{\sharp/\flat}}{p^n - p^{n-1}}$, we have

$$e_n = \mu_* + \frac{\lambda_*}{p^n - p^{n-1}} + \frac{f_{*,n}(v, v_2)}{p^n - p^{n-1}},$$

where $* \in \{\sharp, \flat\}$ is chosen according to the modesty algorithm.

Proof. — From Lemma 6.34 and Lemma 6.35 below, it follows that the valuation matrix of the above expression is a product (of valuation matrices) of the form

$$\left[\mu_\sharp + \frac{\lambda_\sharp}{p^n - p^{n-1}}, \mu_\flat + \frac{\lambda_\flat}{p^n - p^{n-1}}\right] \begin{bmatrix} \frac{f_{\sharp,n}(v,v_2)}{p^n - p^{n-1}} & * \\ \frac{f_{\flat,n}(v,v_2)}{p^n - p^{n-1}} & * \end{bmatrix}$$

except when $v = \frac{p^{-k}}{2}$ and $v_2 = p^{-k}(1 + p^{-1} - p^{-2})$, in which case one of the two entries shown in the right valuation matrix is the actual entry, while the other is a lower estimate, cf. Lemma

[(6)] This has been explicitly done in an unpublished preprint of Greenberg, Iovita, and Pollack.

6.35. The leading term of $P^{\sharp/\flat}(T)$ dominates by assumption, so the Modesty Algorithm 6.28 chooses the correct subindex. *QED*

Lemma 6.33. — *When $v > 0$ and $n > k+3$, the valuation matrix $[\mathcal{H}_a^{n-k-2}(\zeta_{p^n}-1)]$ is*

$$\begin{cases} \begin{bmatrix} p^{2-n}+p^{4-n}+p^{6-n}+\cdots+p^{-k-2} & v+p^{2-n}+\cdots+p^{-k-4} \\ v+p^{1-n}+\cdots+p^{-k-3} & p^{1-n}+\cdots+p^{-k-3} \end{bmatrix} & \text{if } n \equiv k \mod (2) \\ \begin{bmatrix} v+p^{2-n}+\cdots+p^{-k-3} & p^{2-n}+\cdots+p^{-k-3} \\ p^{1-n}+\cdots+p^{-k-2} & v+p^{1-n}+\cdots+p^{-k-4} \end{bmatrix} & \text{if } n \not\equiv k \mod (2). \end{cases}$$

Proof. — Multiplication of valuation matrices and induction. *QED*

Lemma 6.34. — *With notation as above, assume $v = 0$. Then*

$$[\mathcal{H}_a^{n-1}(\zeta_{p^n}-1)] = \begin{bmatrix} 0 & 0 \\ p^{1-n} & p^{1-n} \end{bmatrix}.$$

Proof. — Multiplication of valuation matrices. *QED*

Given a real number x, recall that "$\geqslant x$" denotes an unknown quantity greater than or equal to x.

Lemma 6.35. — *When $v > 0$ and $n > k$, we have $(p^n - p^{n-1})[\mathcal{H}_a^{n-1}(\zeta_{p^n}-1)] =$*

$$\begin{bmatrix} f_{\sharp,n}(v,v_2) & f_{\sharp,n}(v,v_2)-v \\ f_{\flat,n}(v,v_2) & f_{\flat,n}(v,v_2)-v \end{bmatrix} \textit{unless } v = \frac{p^{-k}}{2} \textit{ and } v_2 = 2v(1+p^{-1}-p^{-2}).$$

When $v = \frac{p^{-k}}{2}$ and $v_2 = 2v(1+p^{-1}-p^{-2})$, we have $(p^n-p^{n-1})[\mathcal{H}_a^{n-1}(\zeta_{p^n}-1)] =$

$$\begin{cases} \begin{bmatrix} \geqslant f_{\sharp,n}(v,v_2) & \geqslant f_{\sharp,n}(v,v_2)-v \\ f_{\flat,n}(v,v_2) & f_{\flat,n}(v,v_2)-v \end{bmatrix} & \textit{when } n \equiv k \mod (2) \\ \begin{bmatrix} f_{\sharp,n}(v,v_2) & f_{\sharp,n}(v,v_2)-v \\ \geqslant f_{\flat,n}(v,v_2) & \geqslant f_{\flat,n}(v,v_2)-v \end{bmatrix} & \textit{when } n \not\equiv k \mod (2) \end{cases}$$

Proof. — We give the proof for the case $n \equiv k \mod (2)$ and $n \geqslant k+4$. (The case where $n \not\equiv k \mod 2$ and $n \geqslant 5$ is similar, and the excluded cases are easier variants of these calculations. [7]) We have

$$\mathcal{H}_a^{n-1}(\zeta_{p^n}-1) = \mathcal{H}_a^{n-k-2}(\zeta_{p^n}-1)\mathcal{H}_a^{k+1}(\zeta_{p^n}^{p^{n-k-2}}-1),$$

whose valuation matrix is the product of valuation matrices

$$\left(\begin{bmatrix} \frac{p^{-k}}{p^2-1} & v+\frac{p^{-k-2}}{p^2-1} \\ v+\frac{p^{-k-1}}{p^2-1} & \frac{p^{-k-1}}{p^2-1} \end{bmatrix} - \begin{bmatrix} \frac{p^{2-n}}{p^2-1} & \frac{p^{2-n}}{p^2-1} \\ \frac{p^{1-n}}{p^2-1} & \frac{p^{1-n}}{p^2-1} \end{bmatrix}\right) \begin{bmatrix} v_{k+1} & v_k \\ kv+p^{-1-k} & (k-1)v+p^{-1-k} \end{bmatrix}$$

by Lemma 6.33, where the lower entries in the last valuation matrix are calculated by induction just as in Lemma 6.33 above. The first column of $[\mathcal{H}_a^{n-1}(\zeta_{p^n}-1)]$ is

$$\begin{bmatrix} \min(v_{k+1},(k+1)v+p^{-1-k}-p^{-k-2})+\frac{p^{-k}-p^{2-n}}{p^2-1} \\ \min(v_{k+1},(k-1)v+p^{-1-k})+v+\frac{p^{-k-1}-p^{1-n}}{p^2-1}, \end{bmatrix}$$

[7] For $n = k+1$, we directly verify $[\mathcal{H}_a^k(\zeta_{p^{k+1}}-1)] = \begin{bmatrix} kv & (k-1)v \\ (k-1)v+p^{-k} & (k-2)+p^{-k} \end{bmatrix}$.

as long as the two terms involved in min(,) are different.

If $2v > p^{-k}$, we have $v_{k+1} = (k-1)v + p^{-k}$, so the first column of $[\mathcal{H}_a^{n-1}(\zeta_{p^n} - 1)]$ is

$$\begin{bmatrix} (k-1)v + p^{-k} + \frac{p^{-k}-p^{2-n}}{p^2-1} \\ kv + p^{-1-k} + \frac{p^{-k-1}-p^{1-n}}{p^2-1}. \end{bmatrix}$$

The difficult part is the case $2v = p^{-k}$. From the lemma below, we find that the expression for the lower term is the same as when $2v > p^{-k}$.

We claim that the upper term is the same as well (i.e. the minimum is v_{k+1}) when $v_2 < p^{-k}(1 + \frac{1}{p} - \frac{1}{p^2})$, while the minimum is the other term when $v_2 > p^{-k}(1 + \frac{1}{p} - \frac{1}{p^2})$. For $v_2 \geqslant p^{1-k}$, this follows at once from the below lemma, since $v_{k+1} \geqslant (k-1)v + p^{1-k}$; so the real difficulty is when $p^{1-k} > v_2 \geqslant p^{-k}$: Here, the lemma below tells us that $v_{k+1} = v_2 + (k-1)\frac{p^{-k}}{2}$, from which we obtain our claim. Note that when $v_2 = p^{-k}(1 + \frac{1}{p} - \frac{1}{p^2})$, we obtain our desired inequality. *QED*

Lemma 6.36. — *In the above situation, let $m \geqslant 2$. We then have $v_m = (m-2)v + v_2$ when $v_2 < p^{1-k}$ and $v_m \geqslant (m-2)v + p^{1-k}$ if not.*

Proof. — Explicit decomposition of the valuation matrix of $\mathcal{H}_a^k(\zeta_{p^n}^{p^{n-k-1}} - 1)$. *QED*

A

List of typos in various papers

A.1. Typos in [Po03]:— Note that Pollack writes Φ_{p^n} as Φ_n and ζ_{p^n} as ζ_n.

p. 537, line 2: The term in the sum should be $\zeta_k^{p^{2n-1}t}$, not $\zeta_k^{p^{n-1}t}$.

p. 538, Proof of Lemma 4.5: The displayed formula should be

$$\sup_{|z|_p<r} \left|\Phi_n\left(\gamma^{-j}\cdot(1+z)\right)\right|_p \sim r^{(p-1)p^{n-1}}.$$

p. 538, Lemma 4.6 There is a unit factor missing. The correction is Lemma 2.26.

pg. 539, line 3: Replace the term

$$\frac{1}{p}\prod_{k=1}^{\infty}\frac{\Phi_{2k}(1+T)\cdot(1+T)^{p^{2k-1}(p-1)}}{p} \quad \text{by} \quad \frac{1}{p}\prod_{k=1}^{\infty}\frac{\Phi_{2k}(1+T)/(1+T)^{p^{2k-1}(p-1)}}{p}.$$

p. 541, line 4: "[12,(4.8)] tells us that..." should be "[12,(4.7)] tells us..."

p. 542, Remark 5.3: Note that $\lambda^{\pm}(f_E)$ is defined with Ω_E rather than Ω_{f_E}.

p. 544, Proof of Corollary 5.11: "$L_p(E,\alpha,T)$ is a nonzero function" should be "$L_p(E,\alpha,T)$ can vanish at at most finitely many points of the form $T = \zeta_n - 1$."

p. 545, Theorem 5.13: See Corollary 3.17 in this paper for a corrected statement of the functional equation.

p. 551, penultimate line of Section 6.3: "Lemma 4.8 computes..." instead of "Lemma 4.7 computes..."

p. 552, Definition of $Ш^{an}(E/\mathbb{Q}_n)$: The first term in the fraction should be $L^{(r'_n)}(E//\mathbb{Q}_n)$, where r'_n is the order of vanishing of the complex L-function $L(E/\mathbb{Q}_n, s)$ at $s = 1$.

p. 553, Definition 6.15: $\left[\frac{a}{p^{n+1}}\right]$ should be $\left[\frac{a}{p^{n+1}}\right]^+$.

p. 554, Theorem 6.17*:* This should include the condition that p is supersingular.

p. 554, Line 12: $\omega_n^+ = \prod_{1<2k\leqslant n} \Phi_{2k}(1+T)$, not $\prod_{1\leqslant 2k\leqslant n} \Phi_{2k}(1+T)$.

A.2. Typos in [Ko03]:— *p. 35, Theorem 10.9:* The quantity should be e_n^η, not e_n.

p. 27, Theorem 9.4: $L_p(E, X)$ should be $L_p(E, \alpha, X)$ or $L_p(E, \overline{\alpha}, X)$.

p. 36: Reference 15 is not used in the paper.

A.3. Typos in [PR03]:— *p. 156, line -12:* This should be $[\omega_E, \eta]_{D(E)}$, not $[\omega_E, \eta]_{dR}$. *p. 169, Théorème 6.1 (4)* is slightly inaccurate. See for example [**Sp13**, Section 5] for a corrected version.

A.4. Typo in [LLZ10]:— *p. 40, Lemma 5.23:* The entries are only $O(\log_p^{\frac{1}{2}})$ if $\mathrm{ord}_p(a_p) \geqslant \frac{1}{2}$, cf. Lemma 2.22 in this paper.

A.5. Typo in [Vi76]:— *p. 219, penultimate line:* The term should be

$$S_m(u) = R_0^{(m)}(u) + R_1^{(m)}(u)\log u + \cdots + R_{h-1}^{(m)}(u)\log^{h-1} u.$$

Remark A.1 **(Acknowledgments)**. — We thank our advisors, Barry Mazur, Robert Pollack, and Joseph Silverman, for many inspiring conversations and advice, Christian Wuthrich for a helpful conversation about regulators, and Jay Pottharst for several encouraging comments. We thank Robert Pollack for telling the author about queue sequences, and intentionally withholding his and Adrian Iovita's and Ralph Greenberg's calculation mentioned at the end of the introduction until after we had worked out Theorem 6.29. Finally, we thank Diana Davis and Maxime Bourque for help with typesetting the picture.

References

[AU96] A. Abbes, E. Ullmo: *À propos de la conjecture de Manin pour les courbes elliptiques modulaires*, Compositio Mathematica **103** (1996), no. 3, 269-286.

[AV75] Y. Amice, J. Vélu: *Distributions p-adiques associées aux séries de Hecke*, in Journées Arithmétiques de Bordeaux (Bordeaux, 1974), Astérisque **24-25**, Société Mathématique de France, Montrogue, 1975, 119-131.

[BMS] J. Balakrishnan, J. Müller, W. Stein: *A p-adic analogue of the conjecture of Birch and Swinnerton-Dyer for modular abelian varieties*, arXiv:1210.2739.

[BCDT] C. Breuil, B. Conrad, F. Diamond, and R. Taylor: *On the modularity of elliptic curves over* $\mathbb{Q}$*: Wild 3-adic exercises*, Journal of the American Mathematical Society **14** (2001), 843-939.

[BLZ] L. Berger, H. Li, H. J. Zhu: *Construction of some families of* 2*-dimensional crystalline representations*, Mathematische Annalen **329** (2004), no. 2, 365-377.

[BPR] D. Bernardi, B. Perrin-Riou: *Variante p-adique de la conjecture de Birch et Swinnerton-Dyer (le cas supersingulier)*, Comptes Rendus de l'Académie des Sciences. Paris Série I Mathématique **317** (1993), no. 3, 227-232.

[Co04] Colmez, P.: *La conjecture de Birch et Swinnerton-Dyer p-adique*, Astérisque **294, ix** (2004), 251-319.

[De98] D. Delbourgo: *Iwasawa theory for elliptic curves at unstable primes*, Compositio Mathematica **113** (1998), 123-154.

[Ed91] B. Edixhoven: *On the Manin constants of modular elliptic curves*, Arithmetic Algebraic Geometry, Texel, 1989, Birkhäuser Boston, (1991) 25-39, Boston, MA.

[Gr99] R. Greenberg: *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves, Cetraro, Italy, 1997, Springer Lecture Notes in Mathematics **1716** (1999), 51-144.

[Gr01] R. Greenberg: *Iwasawa theory - past and present*, Class field theory - its centenary and prospect, Tokyo, 1998, Advanced Studies in Pure Mathematics, Mathematical Society of Japan, Tokyo, **30** (2001), 335-385.

[GS94] R. Greenberg, G. Stevens: "On the conjecture of Mazur, Tate, and Teitelbaum" in *p-adic Monodromy and the Birch and Swinnerton-Dyer Conjecture (Boston, 1991)*, Contemporary Mathematics **165**, American Mathematical Society, Providence, 1994, 183 - 211.

[Ka04] K. Kato: *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), 117-290.

[Ke01] K. Kedlaya: *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, Journal of the Ramanujan Mathematical Society, **16** (2001), no. 4, 323-338.

[Ki08] B.D. Kim: *The algebraic functional equation of an elliptic curve at supersingular primes*, Mathematical Research Letters **15**, Issue 1, January 2008.

[Ko03] S. Kobayashi: *Iwasawa theory for elliptic curves at supersingular primes*, Inventiones Mathematicae **152** (2003), no.1, 1-36.

[Ku52] E. Kummer: *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, Journal für die reine und angwandte Mathematik (Crelle's Journal) **44** (1852), 93-146.

[Ku02] M. Kurihara: *On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I*, Inventiones Mathematicae **149** (2002), 195-224.

[KP07] M. Kurihara, R. Pollack: *Two p-adic L-functions and rational points on elliptic curves with supersingular reduction*, L-functions and Galois representations, 300-332, London Mathematical Society Lecture Note Series **320**, Cambridge University Press, Cambridge, 2007.

[KO06] M. Kurihara, R. Otsuki: *On the growth of Selmer groups of an elliptic curve with supersingular reduction in the* $_2$*-extension of* $\mathbb{Q}$, Pure and Applied Mathematics Quarterly **2** (2006), no. 2, part 2, 557-568.

[LLZ10] A. Lei, D. Loeffler, S. Zerbes: *Wach Modules and Iwasawa Theory for Modular Forms*, Asian Journal of Mathematics **14**, no. 4 (December 2010), 475-528.

[LZ] D. Loeffler, S. Zerbes: *Wach modules and critical slope p-adic L-functions*, Journal für die reine und angewandte Mathematik (Crelle's Journal), to appear.

[Ma71] Ju. Manin: *Cyclotomic Fields and Modular Curves*, Uspehi Matematičeskih Nauk **26** (1971), no. 6 (162), 7-71.

[Ma72] Ju Manin: Parabolic points and zeta functions of modular curves, Izvestiya Akademii Nauk SSSR. Seriya Matematičeskaya **36** (1972), 19-66.

[Ma73] Ju. Manin: *Periods of Parabolic Forms and p-adic Hecke series*, Matematičeskii Sbornik, Novaya Seriya **21** (1973), no. 3.

[MST] B. Mazur, W. Stein, J. Tate: *Computation of p-adic heights and log convergence*, Documenta Mathematica 2006, Extra Volume, 577-614.

[MSD] B. Mazur, P. Swinnerton-Dyer: *Arithmetic of Weil curves*, Inventiones Mathematicae **25** (1974), 1-61.

[MTT] B. Mazur, J. Tate, and J. Teitelbaum: *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Inventiones Mathematicae **84** (1986), 1-48.

[PR03] B. Perrin-Riou: *Arithmétique des courbes elliptiques à réduction supersingulière.* Experimental Mathematics **12** (2003), 155-186.

[Po03] R. Pollack: *The p-adic L-function of a modular form at a supersingular prime*, Duke Mathematical Journal **118** (2003), no. 1, 1-36.

[PoSt] R. Pollack, G. Stevens: *Critical slope p-adic L-functions*, Journal of the London Mathematical Society, to appear.

[PW11] R. Pollack and T. Weston: *Mazur-Tate elements of non-ordinary modular forms*, Duke Mathematical Journal, 156 (2011) no. 3, 349–385.

[Ro84] D. Rohrlich: *On L-functions of elliptic curves and cyclotomic towers*, Inventiones Mathematicae **75** (1984), 409-423.

[Ru91] K. Rubin: *The "main conjectures" of Iwasawa theory for imginary quadratic fields*, Inventiones Mathematicae **103** (1991) no.1, 25-68.

[Sh77] G. Shimura: *On the periods of modular forms*, Mathematische Annalen **229** (1977) no. 3, 211-221.

[Si09] J. Silverman: *The Arithmetic of Elliptic Curves*, Second Edition, Graduate Texts in Mathematics **106** (2009), Springer, New York.

[SU] C. Skinner, E. Urban: *The GL_2 Iwasawa Main Conjecture*, submitted.

[Sp12] F. Sprung: *Iwasawa theory for elliptic curves at supersingular primes: A pair of main conjectures*, Journal of Number Theory **132** (2012), no. 7.

[Sp13] F. Sprung: *The Šafarevič-Tate group of an elliptic curve in cyclotomic $_p$-extensions at supersingular primes*, Journal für die reine und angewandte Mathematik (Crelle's Journal), to appear.

[Sp] F. Sprung: *The p-adic L-function of a higher weight modular form*, in preparation.

[SW] W. Stein, C. Wuthrich: *Algorithms for the Arithmetic of Elliptic Curves using Iwasawa Theory*, Mathematics of Computation, to appear.

[Vi76] M. M. Višik: *Nonarchimedean measures associated with Dirichlet series*, Matematičeskii Sbornik **99 (141)**, no. 2 (1976), pp. 248-260, 296.

[Wa80] L. Washington: *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics **83** (1980), Springer, New York.

[Wi95] A. Wiles: *Modular elliptic curves and Fermat's last theorem*, Annals of Mathematics **(2) 141** (1995), 443-551.

Florian Sprung, Brown University, 151 Thayer Street, Providence, RI 02912, USA
E-mail : ian.sprung@gmail.com • *Url :* math.brown.edu/~zeta